# SAINTwriter Exploit Report

**Report Generated: May 8, 2011**

## 1.0 Introduction

On May 7, 2011, at 12:35 PM, a penetration test was conducted using the SAINTexploit™ 7.8 exploit tool. The scan discovered a total of three live hosts, and successfully performed one administrative level exploit, zero user level exploits, zero privilege elevation exploits, and zero client access exploits. The hosts and problems detected are discussed in greater detail in the following sections.

## 2.0 Summary

The following vulnerability severity levels are used to categorize the vulnerabilities:

### REMOTE ADMIN
Vulnerabilities successfully exploited by SAINTexploit to gain remote administrative privileges.

### REMOTE USER
Vulnerabilities successfully exploited by SAINTexploit to gain remote unprivileged access.

### PRIVILEGE ELEVATION
Vulnerabilities successfully exploited by SAINTexploit to gain elevated privileges after gaining remote unprivileged access.

### CLIENT ACCESS
Vulnerabilities successfully exploited due to a user loading an exploit using a client application such as a browser or media player.
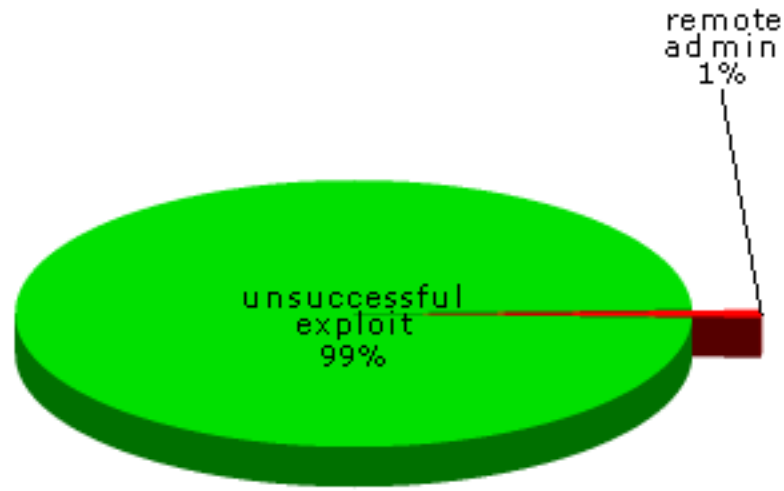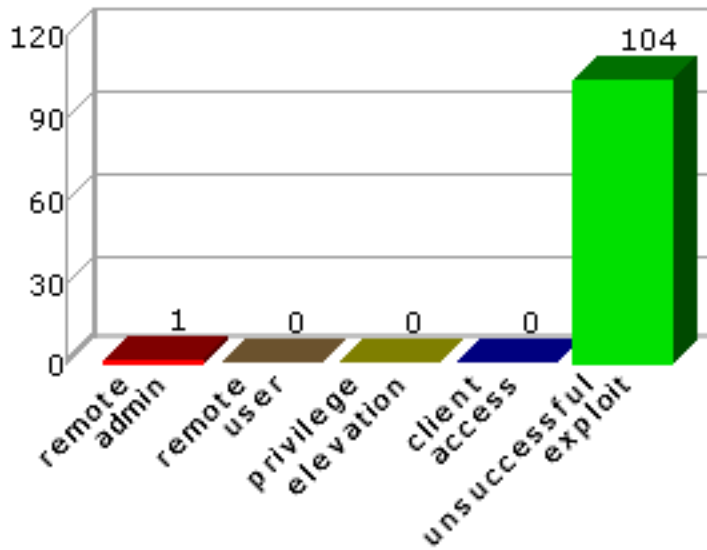
### UNSUCCESSFUL
Vulnerabilities which were not successfully exploited.

The sections below summarize the results of the scan.

## 2.1 Exploited Vulnerabilities by Severity

This section shows the overall number of vulnerabilities exploited at each severity level.

## 2.2 Exploited Hosts by Severity

This section shows the overall number of hosts exploited at each severity level. The severity level of a host is defined as the highest vulnerability severity level exploited on that host.
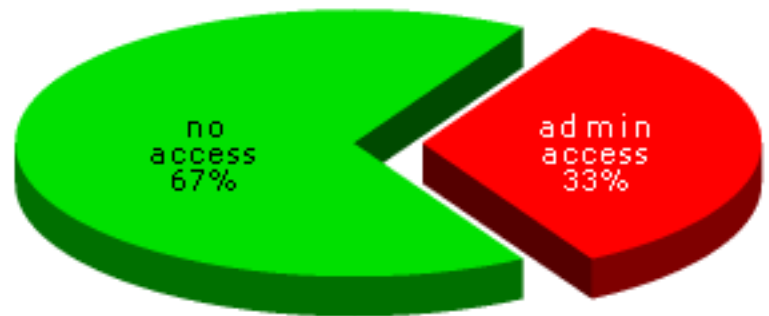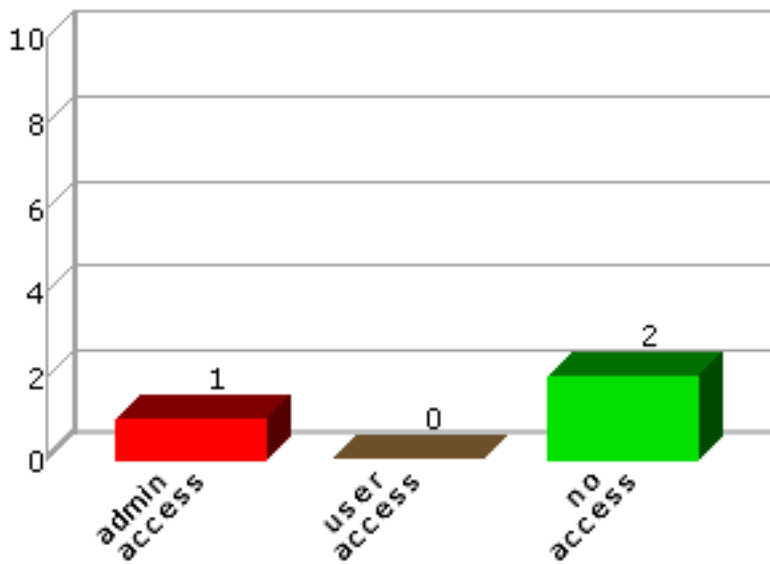


## 2.3 Exploited Vulnerabilities by Class

This section shows the number of vulnerabilities exploited in each of the following classes.

| Class | Description |
| --- | --- |
| Web | Exploits of web servers, CGI programs, and any other software offering an HTTP interface |
| Mail | Exploits of SMTP, IMAP, POP, or web-based mail services |
| File Transfer | Exploits of FTP and TFTP services |
| RPC | Exploits of Remote Procedure Call services |
| Windows OS | Missing hotfixes or vulnerabilities in the registry or SMB shares |
| Passwords | Missing or easily guessed user passwords |

| Browsers | Exploits of web browsers |
|----------|--------------------------|
| **Other** | Any exploit that does not fit into one of the above classes |
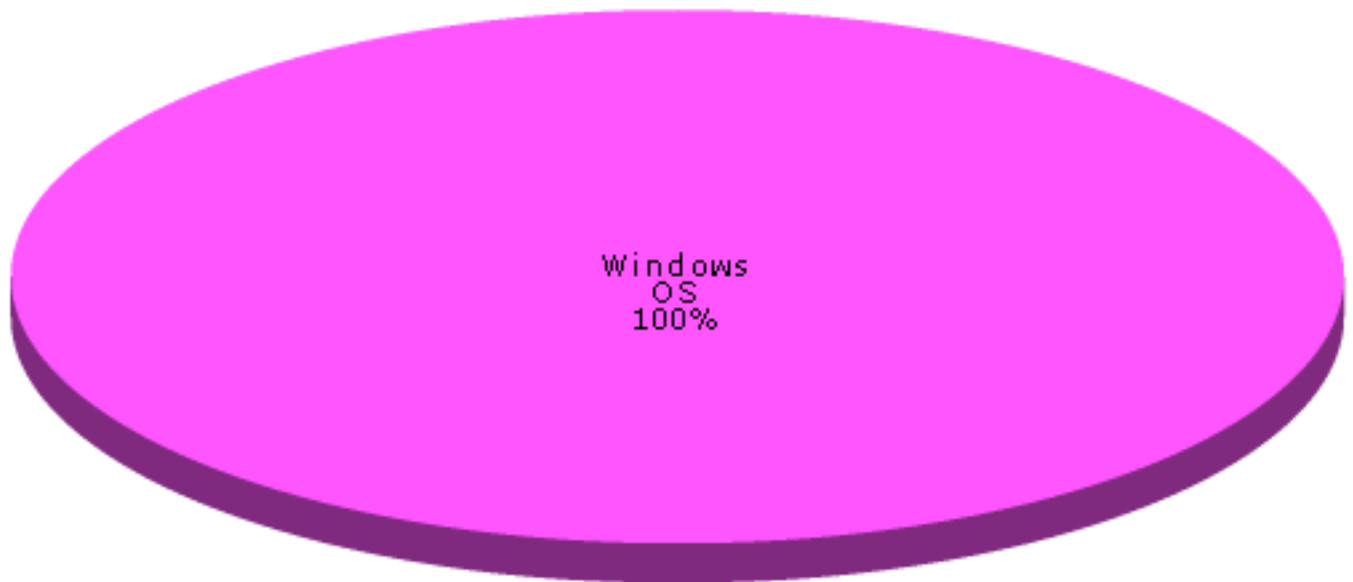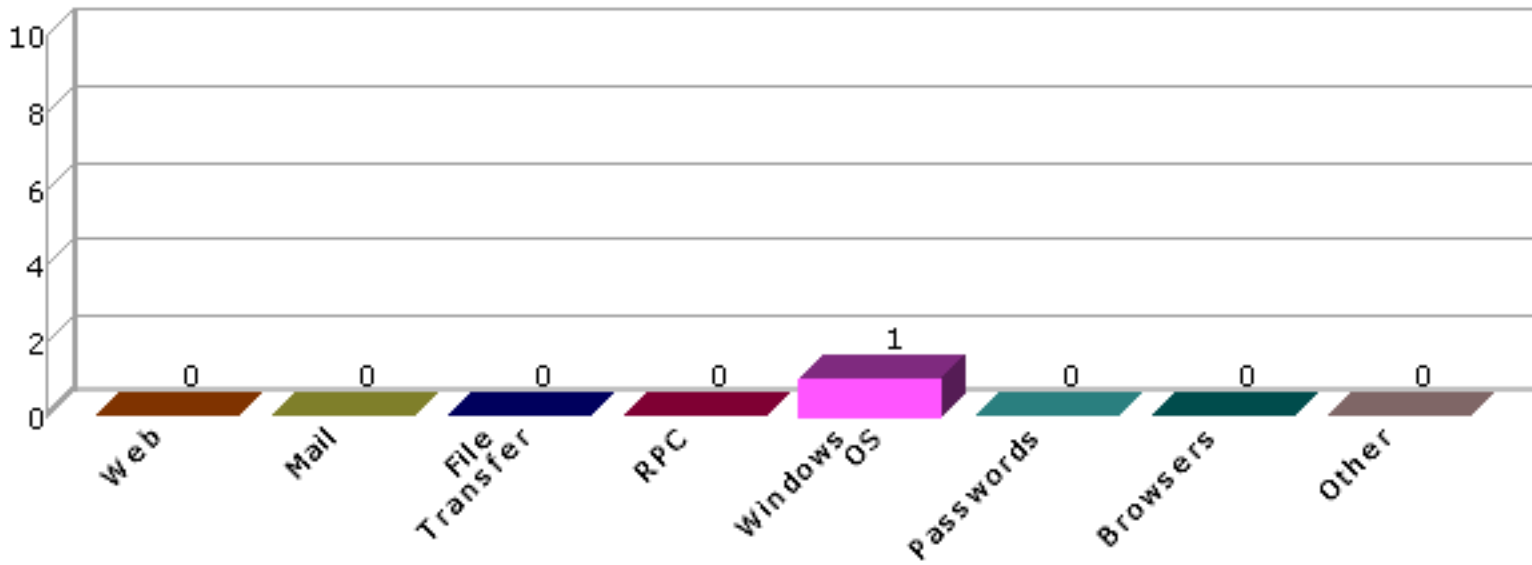




## 2.4 Top 10 Vulnerable Hosts

This section shows the most vulnerable hosts detected, and the number of successful exploits run against them.

| | | |
|---|---|---|
| 1 | 0 | 0 |
| 192.168.0.14 | ls-chl-v2138.local | 192.168.0.12 |
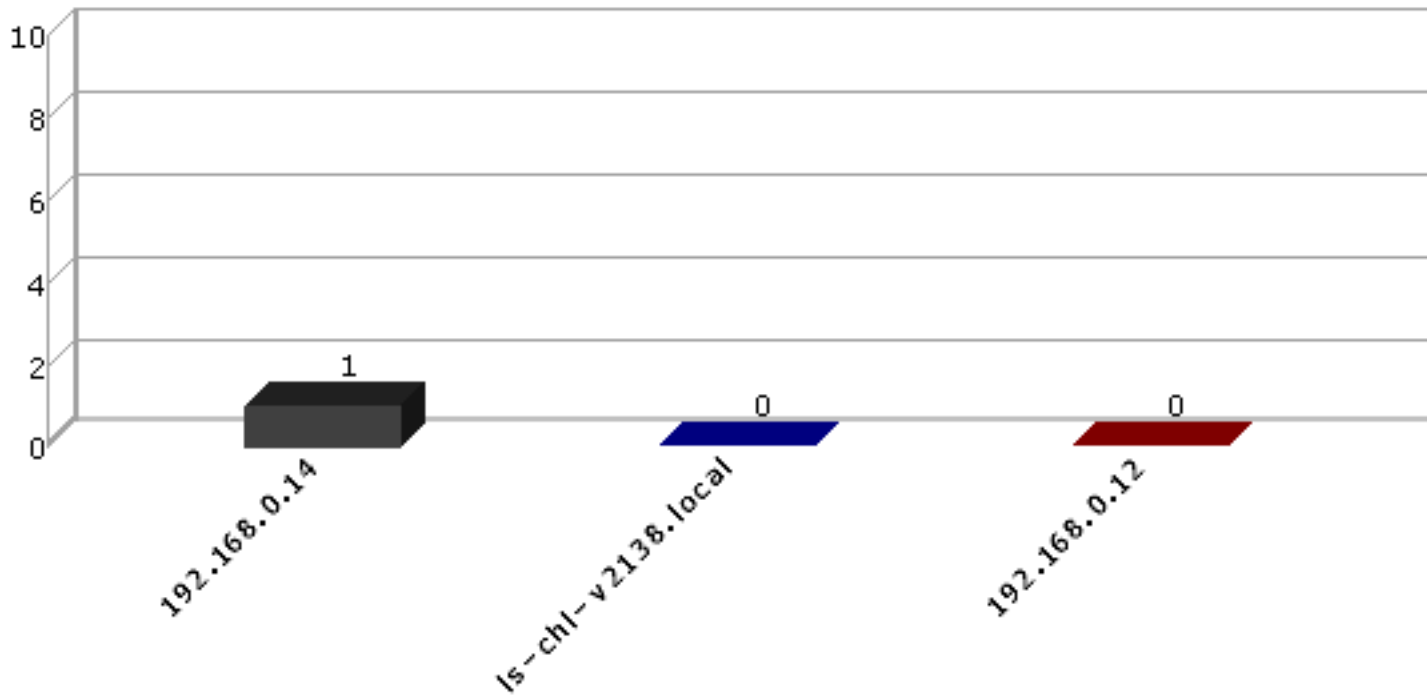
## 2.5 Top 10 Successful Exploits

This section shows the most successful exploits, and the number of hosts against which they succeeded.



Symantec Alert Management System Intel Alert Handler buffer overflow — 2
Snort DCE/RPC preprocessor Windows password weakness — 2
Snort Back Orifice Pre-Processor buffer overflow — 2
HP Data Protector Manager MMD Service Stack Buffer Overflow — 2
Apache Struts2 XWork ParameterInterceptor security bypass — 2
Workstation service NetpManageIPCConnect buffer overflow — 2
Cisco IOS HTTP exec path command execution — 2
Cisco IOS HTTP access level authentication bypass — 2
CS-MARS JBoss jmx-console access — 2

## 2.6 Top 10 Services

This section shows the most common services detected, and the number of hosts on which they were detected.
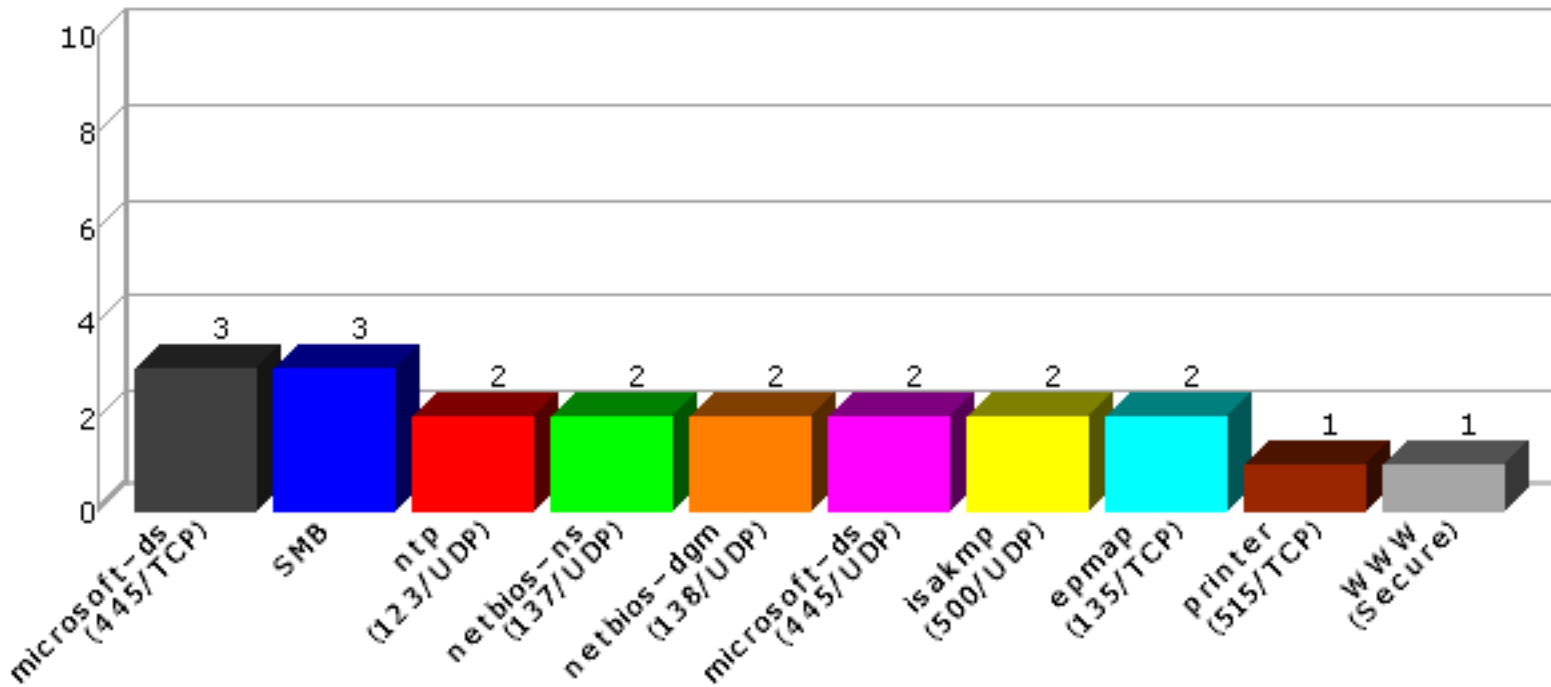
## 3.0 Overview

The following tables present an overview of the hosts discovered on the network and the access level gained on each.

## 3.1 Host List

This table presents an overview of the hosts discovered on the network.

| Host Name | Netbios Name | IP Address | Host Type | Remote Admin | Privilege Elevation | Remote User | Client Access | Unsuccessful Exploits |
|-----------|--------------|------------|-----------|--------------|---------------------|-------------|---------------|-----------------------|
| ls-chl-v2138.local | | 192.168.0.6 | Linux 2.6.22 | 0 | 0 | 0 | 0 | 20 |
| 192.168.0.12 | XP | 192.168.0.12 | Windows XP SP2 | 0 | 0 | 0 | 0 | 68 |
| 192.168.0.14 | 2K3 | 192.168.0.14 | Windows Server 2003 | 1 | 0 | 0 | 0 | 16 |

## 3.2 Exploit List

This table presents an overview of the exploits executed on the network.

| Host Name | Result | Vulnerability / Service | Class | CVE |
|-----------|--------|-------------------------|-------|-----|
| ls-chl-v2138.local | unsuccessful exploit | AWStats configdir parameter command execution | Web | |
| ls-chl-v2138.local | unsuccessful exploit | AWStats migrate parameter command injection | Web | CVE-2006-2237 |

| | | | | |
|---|---|---|---|---|
| ls-chl-v2138.local | unsuccessful exploit | BASE base_qry_common.php file include | Web | CVE-2006-2685 |
| ls-chl-v2138.local | unsuccessful exploit | Cisco IOS HTTP exec path command execution | Web | CVE-2000-0945 |
| ls-chl-v2138.local | unsuccessful exploit | Cisco IOS HTTP access level authentication bypass | Web | CVE-2001-0537 |
| ls-chl-v2138.local | unsuccessful exploit | CS-MARS JBoss jmx-console access | Web | CVE-2006-3733 |
| ls-chl-v2138.local | unsuccessful exploit | Oracle Secure Backup login.php ora_osb_lcookie command execution | Web | |
| ls-chl-v2138.local | unsuccessful exploit | Oracle Secure Backup login.php rbtool command injection | Web | |
| ls-chl-v2138.local | unsuccessful exploit | Oracle Secure Backup property_box.php type parameter command execution | Web | |
| ls-chl-v2138.local | unsuccessful exploit | PHP Remote File Inclusion | Web | |
| ls-chl-v2138.local | unsuccessful exploit | phpBB viewtopic.php highlight parameter vulnerability | Web | |
| ls-chl-v2138.local | unsuccessful exploit | phpRPC decode function command execution | Web | |
| ls-chl-v2138.local | unsuccessful exploit | Samba call_trans2open buffer overflow | Other | |
| ls-chl-v2138.local | unsuccessful exploit | Snort DCE/RPC preprocessor buffer overflow | Other | CVE-2006-5276 |
| ls-chl-v2138.local | unsuccessful exploit | SQL injection | Web | |
| ls-chl-v2138.local | unsuccessful exploit | SQL injection authentication bypass | Web | |
| ls-chl-v2138.local | unsuccessful exploit | TikiWiki file upload vulnerability (jhot.php) | Web | CVE-2006-4602 |
| ls-chl-v2138.local | unsuccessful exploit | Apache Tomcat JK Web Server Connector URI worker map buffer overflow | Web | |
| ls-chl-v2138.local | unsuccessful exploit | TWiki revision control shell command injection | Web | CVE-2005-2877 |
| ls-chl-v2138.local | unsuccessful exploit | TWiki Search.pm shell command injection | Web | CVE-2004-1037 |
| ls-chl-v2138.local | service | 873/TCP | | |
| ls-chl-v2138.local | service | 3689/TCP | | |
| ls-chl-v2138.local | service | 8873/TCP | | |
| ls-chl-v2138.local | service | 9050/TCP | | |
| ls-chl-v2138.local | service | SMB | | |
| ls-chl-v2138.local | service | WWW | | |
| ls-chl-v2138.local | service | WWW (Secure) | | |
| ls-chl-v2138.local | service | WWW (non-standard port 3689) | | |
| ls-chl-v2138.local | service | WWW (non-standard port 9050) | | |
| ls-chl-v2138.local | service | bootpc (68/UDP) | | |
| ls-chl-v2138.local | service | discard (9/UDP) | | |
| ls-chl-v2138.local | service | http (80/TCP) | | |
| ls-chl-v2138.local | service | https (443/TCP) | | |
| ls-chl-v2138.local | service | microsoft-ds (445/TCP) | | |
| ls-chl-v2138.local | service | netbios-ssn (139/TCP) | | |
| ls-chl-v2138.local | service | printer (515/TCP) | | |
| ls-chl-v2138.local | service | tftp (69/UDP) | | |
| ls-chl-v2138.local | info | not vulnerable to cross-site scripting: /webbrowse-e61 /webbrowse-e61/upload | | |
| ls-chl-v2138.local | info | not vulnerable to cross-site scripting: /webbrowse-n95 /webbrowse-n95/upload | | |

| | | | | |
|---|---|---|---|---|
| ls-chl-v2138.local | info | not vulnerable to cross-site scripting: /webbrowse /webbrowse/upload | | |
| 192.168.0.12 | unsuccessful exploit | Adobe Flash Player Flash Content Parsing Code Execution | Other | CVE-2010-3654 |
| 192.168.0.12 | unsuccessful exploit | AWStats migrate parameter command injection | Web | CVE-2006-2237 |
| 192.168.0.12 | unsuccessful exploit | BASE base_qry_common.php file include | Web | CVE-2006-2685 |
| 192.168.0.12 | unsuccessful exploit | CA ARCserve D2D Axis2 default password | Web | CVE-2010-0219 |
| 192.168.0.12 | unsuccessful exploit | CA XOsoft Control Service entry_point.aspx Remote Code Execution | Web | CVE-2010-1223 |
| 192.168.0.12 | unsuccessful exploit | Cisco IOS HTTP exec path command execution | Web | CVE-2000-0945 |
| 192.168.0.12 | unsuccessful exploit | Cisco IOS HTTP access level authentication bypass | Web | CVE-2001-0537 |
| 192.168.0.12 | unsuccessful exploit | CS-MARS JBoss jmx-console access | Web | CVE-2006-3733 |
| 192.168.0.12 | unsuccessful exploit | Easy Chat Server Authentication Request Buffer Overflow | Web | |
| 192.168.0.12 | unsuccessful exploit | Adobe Flash Player authplay.dll vulnerability | Other | CVE-2009-1862 |
| 192.168.0.12 | unsuccessful exploit | Adobe Flash Player callMethod Bytecode Memory Corruption | Other | CVE-2011-0611 |
| 192.168.0.12 | unsuccessful exploit | FrontPage fp30reg.dll remote debug buffer overflow | Web | CVE-2003-0822 |
| 192.168.0.12 | unsuccessful exploit | HP Data Protector Manager MMD Service Stack Buffer Overflow | Other | |
| 192.168.0.12 | unsuccessful exploit | HP Operations Manager hidden Tomcat account | Web | CVE-2009-3843 |
| 192.168.0.12 | unsuccessful exploit | HP OpenView Performance Insight Server Backdoor Account | Web | CVE-2011-0276 |
| 192.168.0.12 | unsuccessful exploit | HP Performance Manager Apache Tomcat Policy Bypass | Web | CVE-2009-3548 |
| 192.168.0.12 | unsuccessful exploit | HP Power Manager formExportDataLogs buffer overflow | Web | CVE-2009-3999 |
| 192.168.0.12 | unsuccessful exploit | HP Power Manager formLogin buffer overflow | Web | CVE-2010-4113 |
| 192.168.0.12 | unsuccessful exploit | HP Power Manager Remote Code Execution | Web | CVE-2009-2685 |
| 192.168.0.12 | unsuccessful exploit | HP Universal CMDB Server Axis2 default password | Web | CVE-2010-0219 |
| 192.168.0.12 | unsuccessful exploit | IBM Rational Quality Manager and Test Lab Manager Policy Bypass | Web | CVE-2010-4094 |
| 192.168.0.12 | unsuccessful exploit | Internet Explorer iepeers.dll use-after-free vulnerability | Browsers | CVE-2010-0806 |
| 192.168.0.12 | unsuccessful exploit | Internet Explorer IFRAME buffer overflow | Browsers | CVE-2004-1050 |
| 192.168.0.12 | unsuccessful exploit | InterSystems Cache HTTP Stack Buffer Overflow | Web | |
| 192.168.0.12 | unsuccessful exploit | RedHat JBoss Enterprise Application Platform JMX Console Authentication Bypass | Web | CVE-2010-0738 |
| 192.168.0.12 | unsuccessful exploit | JRun mod_jrun WriteToLog buffer overflow | Web | CVE-2004-0646 |
| 192.168.0.12 | unsuccessful exploit | Microsoft WMI Administrative Tools ActiveX Control AddContextRef vulnerability | Other | CVE-2010-3973 |
| 192.168.0.12 | unsuccessful exploit | Microsoft Windows Movie Maker IsValidWMToolsStream buffer overflow | Other | CVE-2010-0265 |

| | | | | |
|---|---|---|---|---|
| 192.168.0.12 | unsuccessful exploit | Nagios statuswml.cgi Command Injection | Web | CVE-2009-2288 |
| 192.168.0.12 | unsuccessful exploit | Windows NetDDE buffer overflow | Windows OS | CVE-2004-0206 |
| 192.168.0.12 | unsuccessful exploit | Novell Client NetIdentity Agent XTIERRPCPIPE pointer dereference vulnerability | Other | CVE-2009-1350 |
| 192.168.0.12 | unsuccessful exploit | Novell Client nwspool.dll buffer overflow | Other | CVE-2006-5854 |
| 192.168.0.12 | unsuccessful exploit | Novell Client 4.91 SP4 nwspool.dll buffer overflow | Windows OS | CVE-2007-6701 |
| 192.168.0.12 | unsuccessful exploit | Novell iManager EnteredClassName buffer overflow | Web | CVE-2010-1929 |
| 192.168.0.12 | unsuccessful exploit | Novell iManager getMultiPartParameters file upload vulnerability | Web | |
| 192.168.0.12 | unsuccessful exploit | HP OpenView Network Node Manager getnnmdata.exe CGI Hostname buffer overflow | Web | CVE-2010-1555 |
| 192.168.0.12 | unsuccessful exploit | HP OpenView NNM getnnmdata.exe CGI ICount Parameter Buffer Overflow | Web | CVE-2010-1554 |
| 192.168.0.12 | unsuccessful exploit | HP OpenView Network Node Manager getnnmdata.exe CGI MaxAge buffer overflow | Web | CVE-2010-1553 |
| 192.168.0.12 | unsuccessful exploit | HP OpenView Network Node Manager malformed displayWidth option to jovgraph.exe | Web | CVE-2011-0261 |
| 192.168.0.12 | unsuccessful exploit | HP OpenView Network Node Manager nnmRptConfig.exe CGI Template Buffer Overflow | Web | CVE-2009-3848 |
| 192.168.0.12 | unsuccessful exploit | HP OpenView Network Node Manager nnmRptConfig.exe nameParams text1 Buffer Overflow | Web | CVE-2011-0268 |
| 192.168.0.12 | unsuccessful exploit | HP OpenView Network Node Manager nnmRptConfig.exe schd_select1 Remote Code Execution | Web | CVE-2011-0269 |
| 192.168.0.12 | unsuccessful exploit | HP OpenView Network Node Manager OpenView5.exe buffer overflow | Web | CVE-2008-0067 |
| 192.168.0.12 | unsuccessful exploit | HP OpenView Network Node Manager ovalarm.exe Accept-Language buffer overflow | Web | CVE-2009-4179 |
| 192.168.0.12 | unsuccessful exploit | HP OpenView Network Node Manager ovlogin.exe buffer overflow | Web | CVE-2007-6204 |
| 192.168.0.12 | unsuccessful exploit | HP OpenView Network Node Manager ovwebsnmpsrv.exe buffer overflow via jovgraph.exe | Web | CVE-2009-4181 |
| 192.168.0.12 | unsuccessful exploit | HP OpenView Network Node Manager snmpviewer.exe CGI Stack Buffer Overflow | Web | CVE-2010-1552 |
| 192.168.0.12 | unsuccessful exploit | HP OpenView Network Node Manager Toolbar.exe CGI buffer overflow | Web | CVE-2008-0067 |
| 192.168.0.12 | unsuccessful exploit | Serv-U Web Client session cookie handling buffer overflow | Web | |
| 192.168.0.12 | unsuccessful exploit | Windows password weakness | Passwords | CVE-1999-0503 |
| 192.168.0.12 | unsuccessful exploit | Snort Back Orifice Pre-Processor buffer overflow | Other | CVE-2005-3252 |
| 192.168.0.12 | unsuccessful exploit | Snort DCE/RPC preprocessor buffer overflow | Other | CVE-2006-5276 |
| 192.168.0.12 | unsuccessful exploit | Apache Struts2 XWork ParameterInterceptor security bypass | Web | CVE-2010-1870 |
| 192.168.0.12 | unsuccessful exploit | Symantec Alert Management System Intel Alert Handler command execution | Other | |
| 192.168.0.12 | unsuccessful exploit | TikiWiki file upload vulnerability (jhot.php) | Web | CVE-2006-4602 |
| 192.168.0.12 | unsuccessful exploit | Trend Micro OfficeScan cgiRecvFile.exe ComputerName buffer overflow | Web | CVE-2008-2437 |

| | | | | |
|---|---|---|---|---|
| 192.168.0.12 | unsuccessful exploit | Trend Micro OfficeScan Policy Server CGI buffer overflow | Web | CVE-2008-1365 |
| 192.168.0.12 | unsuccessful exploit | TWiki revision control shell command injection | Web | CVE-2005-2877 |
| 192.168.0.12 | unsuccessful exploit | TWiki Search.pm shell command injection | Web | CVE-2004-1037 |
| 192.168.0.12 | unsuccessful exploit | Windows LSASS buffer overflow | Windows OS | CVE-2003-0533 |
| 192.168.0.12 | unsuccessful exploit | Windows Plug and Play buffer overflow | Windows OS | CVE-2005-1983 |
| 192.168.0.12 | unsuccessful exploit | Windows RPC DCOM interface buffer overflow | Windows OS | CVE-2003-0352 |
| 192.168.0.12 | unsuccessful exploit | Windows RRAS memory corruption vulnerability | Windows OS | CVE-2006-2370 |
| 192.168.0.12 | unsuccessful exploit | Windows Server Service buffer overflow | Windows OS | CVE-2006-3439 |
| 192.168.0.12 | unsuccessful exploit | Windows Server Service buffer overflow MS08-067 | Windows OS | CVE-2008-4250 |
| 192.168.0.12 | unsuccessful exploit | Windows Thumbnail View CreateSizedDIBSECTION buffer overflow | Windows OS | CVE-2010-3970 |
| 192.168.0.12 | unsuccessful exploit | Windows Workstation service NetpManageIPCConnect buffer overflow | Windows OS | CVE-2006-4691 |
| 192.168.0.12 | unsuccessful exploit | Wireshark LWRES dissector buffer overflow | Other | CVE-2010-0304 |
| 192.168.0.12 | service | 1900/UDP | | |
| 192.168.0.12 | service | SMB | | |
| 192.168.0.12 | service | WWW (non-standard port 2869) | | |
| 192.168.0.12 | service | epmap (135/TCP) | | |
| 192.168.0.12 | service | isakmp (500/UDP) | | |
| 192.168.0.12 | service | microsoft-ds (445/TCP) | | |
| 192.168.0.12 | service | microsoft-ds (445/UDP) | | |
| 192.168.0.12 | service | netbios-dgm (138/UDP) | | |
| 192.168.0.12 | service | netbios-ns (137/UDP) | | |
| 192.168.0.12 | service | ntp (123/UDP) | | |
| 192.168.0.14 | remote admin | Windows RPC DCOM interface buffer overflow | Windows OS | CVE-2003-0352 |
| 192.168.0.14 | unsuccessful exploit | Computer Associates Alert Notification Server buffer overflow | Other | CVE-2007-3825 |
| 192.168.0.14 | unsuccessful exploit | Computer Associates Alert Notification Server opcode 23 buffer overflow | Other | CVE-2007-4620 |
| 192.168.0.14 | unsuccessful exploit | HP Data Protector Manager MMD Service Stack Buffer Overflow | Other | |
| 192.168.0.14 | unsuccessful exploit | Windows NetDDE buffer overflow | Windows OS | CVE-2004-0206 |
| 192.168.0.14 | unsuccessful exploit | Novell Client NetIdentity Agent XTIERRPCPIPE pointer dereference vulnerability | Other | CVE-2009-1350 |
| 192.168.0.14 | unsuccessful exploit | Novell Client nwspool.dll buffer overflow | Other | CVE-2006-5854 |
| 192.168.0.14 | unsuccessful exploit | Novell Client nwspool.dll EnumPrinters buffer overflow | Other | CVE-2008-0639 |
| 192.168.0.14 | unsuccessful exploit | Novell Client 4.91 SP4 nwspool.dll buffer overflow | Windows OS | CVE-2007-6701 |
| 192.168.0.14 | unsuccessful exploit | Windows password weakness | Passwords | CVE-1999-0503 |
| 192.168.0.14 | unsuccessful exploit | Snort Back Orifice Pre-Processor buffer overflow | Other | CVE-2005-3252 |

| | | | | |
|---|---|---|---|---|
| 192.168.0.14 | unsuccessful exploit | Apache Struts2 XWork ParameterInterceptor security bypass | Web | CVE-2010-1870 |
| 192.168.0.14 | unsuccessful exploit | Symantec Alert Management System Intel Alert Handler command execution | Other | |
| 192.168.0.14 | unsuccessful exploit | Windows DNS server RPC management interface buffer overflow | RPC | CVE-2007-1748 |
| 192.168.0.14 | unsuccessful exploit | Windows Plug and Play buffer overflow | Windows OS | CVE-2005-1983 |
| 192.168.0.14 | unsuccessful exploit | Windows Server Service buffer overflow MS08-067 | Windows OS | CVE-2008-4250 |
| 192.168.0.14 | unsuccessful exploit | Windows Workstation service NetpManageIPCConnect buffer overflow | Windows OS | CVE-2006-4691 |
| 192.168.0.14 | service | 1025/TCP | | |
| 192.168.0.14 | service | 1026/TCP | | |
| 192.168.0.14 | service | 1028/UDP | | |
| 192.168.0.14 | service | SMB | | |
| 192.168.0.14 | service | epmap (135/TCP) | | |
| 192.168.0.14 | service | isakmp (500/UDP) | | |
| 192.168.0.14 | service | microsoft-ds (445/TCP) | | |
| 192.168.0.14 | service | microsoft-ds (445/UDP) | | |
| 192.168.0.14 | service | netbios-dgm (138/UDP) | | |
| 192.168.0.14 | service | netbios-ns (137/UDP) | | |
| 192.168.0.14 | service | ntp (123/UDP) | | |
| 192.168.0.14 | info | Found password hash: Administrator : 500 : 4bd0f3d13d038cc3935d0e10d22e87c7 : bd09d74cbc4777b88b0ea5a7df135b03 | | |
| 192.168.0.14 | info | Found password hash: Guest : 501 : 31d6cfe0d16ae931b73c59d7e0c089c0 : aad3b435b51404eeaad3b435b51404ee | | |
| 192.168.0.14 | info | Found password hash: SUPPORT_388945a0 : 1001 : 5502b52ab1b5d056655969b871c44809 : aad3b435b51404eeaad3b435b51404ee | | |

## 4.0 Details

The following sections provide details on the specific exploits executed on each host.

## 4.1 ls-chl-v2138.local

**IP Address:** 192.168.0.6
**Scan time:** May 07 12:35:06 2011

**Host type:** Linux 2.6.22

### AWStats configdir parameter command execution

**Severity:** Unsuccessful Exploit

**Resolution**

Upgrade to AWStats 6.3 or higher.

**References**

http://www.idefense.com/intelligence/vulnerabilities/display.php?id=185&type=vulnerabilities

**Limitations**

Exploit works on AWStats 6.2 on Linux.

## AWStats migrate parameter command injection

**Severity:** Unsuccessful Exploit                    **CVE:**   CVE-2006-2237

**Resolution**

Upgrade to AWStats 6.6 or higher, or disable the `AllowToUpdateStatsFromBrowser` option in the AWStats configuration file.

**References**

http://secunia.com/advisories/19969

## BASE base_qry_common.php file include

**Severity:** Unsuccessful Exploit                    **CVE:**   CVE-2006-2685

**Resolution**

Upgrade to BASE 1.2.5 or higher.

**References**

http://secunia.com/advisories/20300

**Limitations**

In order for this exploit to succeed, the register_globals option must be enabled in the PHP configuration, and the Apache log file must exist in a common location.

## Cisco IOS HTTP exec path command execution

**Severity:** Unsuccessful Exploit                    **CVE:**   CVE-2000-0945

**Resolution**

Set an enable password on the Cisco device.

**References**

http://archives.neohapsis.com/archives/bugtraq/2000-10/0380.html
http://archives.neohapsis.com/archives/bugtraq/2000-11/0194.html

**Limitations**

Exploit works on Cisco Catalyst 3500 XL devices with the enable password unset.

## Cisco IOS HTTP access level authentication bypass

**Severity:** Unsuccessful Exploit                    **CVE:**   CVE-2001-0537

**Resolution**

Apply the fix referenced in cisco-sa-20010627-ios-http-level. Alternatively, disable the HTTP interface or use TACACS+ or Radius for authentication.

**References**

http://www.cert.org/advisories/CA-2001-14.html

**Limitations**

Exploit works on Cisco IOS 11.3 through 12.2.

The target must have the HTTP interface enabled and be using local authentication in order for the exploit to succeed.

## CS-MARS JBoss jmx-console access

**Severity:** Unsuccessful Exploit                    **CVE:**   CVE-2006-3733

**Resolution**

Upgrade to CS-MARS 4.2.1 or higher or apply the upgrade referenced in Cisco Security Advisory cisco-sa-20060719-mars.

**References**

http://www.securityfocus.com/archive/1/440641

## Oracle Secure Backup login.php ora_osb_lcookie command execution

**Severity:** Unsuccessful Exploit

**Resolution**

Apply the patch referenced in the Oracle Critical Patch Update for January 2009.

**References**

http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=768

**Limitations**

Exploit works on Oracle Secure Backup 10.1.0.3.

When exploiting Windows targets, SAINTexploit must be able to bind to port 69/UDP.

When exploiting Linux targets, the "nc" utility must be installed on the target platform.

The IO-Socket-SSL PERL module is required for this exploit to run. This module is available from http://www.cpan.org/modules/by-module/IO/.

## Oracle Secure Backup login.php rbtool command injection

**Severity:** Unsuccessful Exploit

## Resolution

Apply the patch referenced in the Oracle Critical Patch Update Advisory - January 2009.

## References

http://www.zerodayinitiative.com/advisories/ZDI-09-003/

## Limitations

Exploit works on Oracle Secure Backup 10.1.0.3.

The IO-Socket-SSL PERL module is required for this exploit to run. This module is available from http://www.cpan.org/modules/by-module/IO/.

When the target is Windows, this exploit must be able to bind to port 69/UDP in order to succeed.

When the target is Linux, the target must have the "nc" utility in order for the exploit to succeed.

## Oracle Secure Backup property_box.php type parameter command execution

**Severity:** Unsuccessful Exploit

## Resolution

Apply the patch referenced in the Oracle Critical Patch Update for July 2009.

## References

http://www.securityfocus.com/bid/35678

## Limitations

Exploit works on Oracle Secure Backup 10.2.0.3.

When the target is Windows, this exploit must be able to bind to port 69/UDP in order to succeed.

When exploiting Linux targets, the netcat ("nc") utility must be installed on the target platform.

The IO-Socket-SSL PERL module is required for this exploit to run. This module is available from http://www.cpan.org/modules/by-module/IO/.

## PHP Remote File Inclusion

**Severity:** Unsuccessful Exploit

## Resolution

Fix the vulnerable code so that included path names cannot be manipulated by the user.

The vulnerability can also be mitigated by setting the following variables in the PHP configuration file:

```
register_globals = Off
allow_url_include = Off
```

safe_mode = On

**References**

http://projects.webappsec.org/Remote-File-Inclusion

**Limitations**

This exploit works against Unix and Linux operating systems.

The exploit requires the `register_globals` and `allow_url_include` PHP settings to be on, and the `safe_mode` PHP setting to be off.

The `telnet` and `mkfifo` programs must exist on the target in order for the shell connection to be established.

## phpBB viewtopic.php highlight parameter vulnerability

**Severity:** Unsuccessful Exploit

**Resolution**

Upgrade to the latest version of phpBB.

**References**

http://archives.neohapsis.com/archives/bugtraq/2005-06/0256.html

## phpRPC decode function command execution

**Severity:** Unsuccessful Exploit

**Resolution**

phpRPC is no longer maintained by the author, so no fix is available. If phpRPC is installed as part of another product, contact the vendor of that product for a fix. Otherwise, remove phpRPC from the server.

**References**

http://archives.neohapsis.com/archives/bugtraq/2006-02/0507.html

## Samba call_trans2open buffer overflow

**Severity:** Unsuccessful Exploit

**Resolution**

Upgrade to Samba 2.2.8a or higher.

**References**

http://www.kb.cert.org/vuls/id/267873
http://archives.neohapsis.com/archives/bugtraq/2003-04/0100.html

**Limitations**

Exploit works on Samba 2.2.x.

## Snort DCE/RPC preprocessor buffer overflow

**Severity:** Unsuccessful Exploit          **CVE:**   CVE-2006-5276

### Resolution

Upgrade to Snort 2.6.1.3 or higher.

### References

http://www.us-cert.gov/cas/techalerts/TA07-050A.html
http://www.snort.org/docs/advisory-2007-02-19.html

### Limitations

Exploit works on Snort 2.6.1.1 on Windows and Snort 2.6.1.2 on Red Hat 8, and requires port 445/TCP to be open on the target.

## SQL injection

**Severity:** Unsuccessful Exploit

### Resolution

Modify the web program to remove invalid characters from input parameters before using them in SQL queries.

### References

http://www.windowsecurity.com/whitepapers/What-SQL-Injection.html

### Limitations

Exploit works on MySQL, Oracle Database, and Microsoft SQL Server.

In order for the exploit to succeed, the vulnerable parameter must be present in an HTML form which is accessible by following links from the home page of a web site. The web program must display the result of the affected query somewhere in the response page. The success of the exploit may also depend on the structure of the affected query.

If using the https protocol, the exploit requires the IO-Socket-SSL PERL module to be installed on the scanning host. This module is available from http://www.cpan.org/modules/by-module/IO/.

## SQL injection authentication bypass

**Severity:** Unsuccessful Exploit

### Resolution

Modify the web program to remove invalid characters from input parameters before using them in SQL queries.

### References

http://www.windowsecurity.com/whitepapers/What-SQL-Injection.html

**Limitations**

In order for the exploit to succeed, the login form must be accessible by following links from the home page of a web site. The web program must allow authentication based on the response of a simple username and password query.

If using the https protocol, the exploit requires the IO-Socket-SSL PERL module to be installed on the scanning host. This module is available from http://www.cpan.org/modules/by-module/IO/.

---

## TikiWiki file upload vulnerability (jhot.php)

**Severity:** Unsuccessful Exploit        **CVE:**  CVE-2006-4602

**Resolution**

Upgrade to TikiWiki 1.9.5 or higher.

**References**

http://secunia.com/advisories/21733

---

## Apache Tomcat JK Web Server Connector URI worker map buffer overflow

**Severity:** Unsuccessful Exploit

**Resolution**

Upgrade to mod_jk 1.2.21 or higher.

**References**

http://tomcat.apache.org/security-jk.html
http://www.zerodayinitiative.com/advisories/ZDI-07-008/

**Limitations**

Exploit works on Apache Tomcat JK Web Server Connector 1.2.19 for Apache HTTP Server 2.0.58 on Windows and Apache Tomcat JK Web Server Connector 1.2.20 for Apache HTTP Server 2.0.58 on Linux. Apache, Apache Tomcat, and the JK Web Server Connector must be properly configured on the target in order for this exploit to succeed.

IPv6 support for this exploit is only available for Linux targets.

---

## TWiki revision control shell command injection

**Severity:** Unsuccessful Exploit        **CVE:**  CVE-2005-2877

**Resolution**

Apply the patch referenced in CIAC Bulletin P-307.

**References**

http://archives.neohapsis.com/archives/bugtraq/2005-09/0154.html

## TWiki Search.pm shell command injection

**Severity:** Unsuccessful Exploit          **CVE:**   CVE-2004-1037

**Resolution**

Apply the update referenced in CIAC Bulletin P-039.

**References**

http://archives.neohapsis.com/archives/bugtraq/2004-11/0181.html

## 873/TCP
**Severity:** Service

## 3689/TCP
**Severity:** Service

## 8873/TCP
**Severity:** Service

## 9050/TCP
**Severity:** Service

## SMB
**Severity:** Service

## WWW
**Severity:** Service

## WWW (Secure)
**Severity:** Service

## WWW (non-standard port 3689)
**Severity:** Service

## WWW (non-standard port 9050)
**Severity:** Service

## bootpc (68/UDP)
**Severity:** Service

## discard (9/UDP)
**Severity:** Service

## http (80/TCP)
**Severity:** Service

## https (443/TCP)
**Severity:** Service

## microsoft-ds (445/TCP)
**Severity:** Service

## netbios-ssn (139/TCP)
**Severity:** Service

## printer (515/TCP)
**Severity:** Service

## tftp (69/UDP)
**Severity:** Service

## 4.2 192.168.0.12

**IP Address:** 192.168.0.12
**Scan time:** May 02 05:23:02 2011

**Host type:** Windows XP SP2
**Netbios Name:** XP

## Adobe Flash Player Flash Content Parsing Code Execution

| | |
|---|---|
| **Severity:** Unsuccessful Exploit | **CVE:** CVE-2010-3654 |

### Resolution

Apply the patches referenced in APSA10-05 when they become available. In the interim, follow the relevant directions for mitigating the vulnerability in Adobe Reader.

### References

http://www.kb.cert.org/vuls/id/298081
http://secunia.com/advisories/42030/

### Limitations

Exploit works on Adobe Reader 9.4.0 and the user must open the exploit file in Adobe Reader.

## AWStats migrate parameter command injection

| | |
|---|---|
| **Severity:** Unsuccessful Exploit | **CVE:** CVE-2006-2237 |

### Resolution

Upgrade to AWStats 6.6 or higher, or disable the `AllowToUpdateStatsFromBrowser` option in the AWStats configuration file.

### References

http://secunia.com/advisories/19969

## BASE base_qry_common.php file include

**Severity:** Unsuccessful Exploit  **CVE:** CVE-2006-2685

### Resolution

Upgrade to BASE 1.2.5 or higher.

### References

http://secunia.com/advisories/20300

### Limitations

In order for this exploit to succeed, the register_globals option must be enabled in the PHP configuration, and the Apache log file must exist in a common location.

---

## CA ARCserve D2D Axis2 default password

**Severity:** Unsuccessful Exploit  **CVE:** CVE-2010-0219

### Resolution

Change the password for the admin account in the axis2.xml file, which is found in the \Program Files\CA\ARCserve D2D\TOMCAT\webapps\WebServiceImpl\WEB-INF\conf folder.

### References

http://www.securityfocus.com/archive/1/515494

### Limitations

Exploit works on CA ARCserve D2D r15.

There may be a delay before the exploit succeeds.

---

## CA XOsoft Control Service entry_point.aspx Remote Code Execution

**Severity:** Unsuccessful Exploit  **CVE:** CVE-2010-1223

### Resolution

Apply the patches referenced in CA Security Notice for CA XOsoft CA20100406-01.

### References

http://secunia.com/advisories/39337/

### Limitations

Exploit works on CA XOsoft Control Service r12.5.

---

## Cisco IOS HTTP exec path command execution

**Severity:** Unsuccessful Exploit  **CVE:** CVE-2000-0945

### Resolution

Set an enable password on the Cisco device.

**References**

http://archives.neohapsis.com/archives/bugtraq/2000-10/0380.html
http://archives.neohapsis.com/archives/bugtraq/2000-11/0194.html

**Limitations**

Exploit works on Cisco Catalyst 3500 XL devices with the enable password unset.

## Cisco IOS HTTP access level authentication bypass

**Severity:** Unsuccessful Exploit                **CVE:**  CVE-2001-0537

**Resolution**

Apply the fix referenced in cisco-sa-20010627-ios-http-level. Alternatively, disable the HTTP interface or use TACACS+ or Radius for authentication.

**References**

http://www.cert.org/advisories/CA-2001-14.html

**Limitations**

Exploit works on Cisco IOS 11.3 through 12.2.

The target must have the HTTP interface enabled and be using local authentication in order for the exploit to succeed.

## CS-MARS JBoss jmx-console access

**Severity:** Unsuccessful Exploit                **CVE:**  CVE-2006-3733

**Resolution**

Upgrade to CS-MARS 4.2.1 or higher or apply the upgrade referenced in Cisco Security Advisory cisco-sa-20060719-mars.

**References**

http://www.securityfocus.com/archive/1/440641

## Easy Chat Server Authentication Request Buffer Overflow

**Severity:** Unsuccessful Exploit

**Resolution**

Easy Chat Server 2.2 and earlier are vulnerable. Contact the vendor at support@echatserver.com for information on when a fix will be available.

**References**

http://milw0rm.com/exploits/8142
http://securitytracker.com/alerts/2009/Mar/1021785.html

**Limitations**

Exploit works on Easy Chat Server 2.2 on Windows 2000 and Windows 2003.

## Adobe Flash Player authplay.dll vulnerability

**Severity:** Unsuccessful Exploit          **CVE:**  CVE-2009-1862

**Resolution**

Apply the update referenced in APSB09-10.

**References**

http://www.adobe.com/support/security/advisories/apsa09-03.html
http://www.kb.cert.org/vuls/id/259425

**Limitations**

Exploit works on Flash Player 10.0.22.87 and requires a user to load the exploit page into Internet Explorer 6 or 7.

After a user loads the exploit page, there may be a delay before the exploit succeeds.

## Adobe Flash Player callMethod Bytecode Memory Corruption

**Severity:** Unsuccessful Exploit          **CVE:**  CVE-2011-0611

**Resolution**

Upgrade to Adobe Flash Player 10.2.153.2 for Windows or higher.

**References**

http://www.adobe.com/support/security/advisories/apsa11-02.html
http://secunia.com/advisories/44119/

**Limitations**

Exploit works on Adobe Systems Flash Player 10.2.153.1. The targeted user must open the exploit file in Internet Explorer 7.

## FrontPage fp30reg.dll remote debug buffer overflow

**Severity:** Unsuccessful Exploit          **CVE:**  CVE-2003-0822

**Resolution**

Apply the patch referenced in Microsoft Security Bulletin 03-051.

**References**

## HP Data Protector Manager MMD Service Stack Buffer Overflow

**Severity:** Unsuccessful Exploit

### Resolution

Apply a patch when it becomes available.

### References

http://secunia.com/advisories/41735

### Limitations

Exploit works on HP Data Protector Media Operations 6.11.

The Media Management Daemon service uses a dynamically assigned TCP port in the range 1024 to 65535.

## HP Operations Manager hidden Tomcat account

**Severity:** Unsuccessful Exploit          **CVE:**  CVE-2009-3843

### Resolution

Apply the patch referenced in HPSBMA02478 SSRT090251.

### References

http://www.zerodayinitiative.com/advisories/ZDI-09-085/

### Limitations

Exploit works on HP Operations Manager A.08.10 on Windows Server 2003 and Windows Server 2008.

## HP OpenView Performance Insight Server Backdoor Account

**Severity:** Unsuccessful Exploit          **CVE:**  CVE-2011-0276

### Resolution

Apply patch 5.41.002 piweb HF02.

### References

http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c02695453
http://secunia.com/advisories/43145
http://osvdb.org/70754
http://www.securityfocus.com/bid/46079

### Limitations

This exploit works against HP OpenView Performance Insight (OVPI) 5.41.0 on Windows Server 2003 SP2 English (DEP OptOut) and Windows Server 2008 SP1 English (DEP OptOut).

## HP Performance Manager Apache Tomcat Policy Bypass

**Severity:** Unsuccessful Exploit          **CVE:**   CVE-2009-3548

### Resolution

Apply the fix referenced in HP Security Bulletin HPSBMA02535.

### References

http://secunia.com/advisories/39847/

### Limitations

Exploit works on HP Performance Manager 8.1 on Microsoft Windows Server 2003 and Windows Server 2008.

It may take longer than usual to establish the connection after successful exploitation because it takes time for the affected server to deploy the malicious WAR file.

## HP Power Manager formExportDataLogs buffer overflow

**Severity:** Unsuccessful Exploit          **CVE:**   CVE-2009-3999

### Resolution

Upgrade to HP Power Manager 4.2.10 or higher.

### References

http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c01971741
http://secunia.com/secunia_research/2009-47/

### Limitations

Exploit works on HP Power Manager 4.2.9 on Microsoft Windows Server 2003 SP2 with patch KB933729.

## HP Power Manager formLogin buffer overflow

**Severity:** Unsuccessful Exploit          **CVE:**   CVE-2010-4113

### Resolution

Upgrade to HP Power Manager 4.3.2.

### References

http://www.securityfocus.com/archive/1/515283

### Limitations

Exploit works on HP Power Manager 4.2.10 on Windows Server 2003 SP2 with KB956802 and KB956572.

## HP Power Manager Remote Code Execution

**Severity:** Unsuccessful Exploit          **CVE:**   CVE-2009-2685

## Resolution

HP's resolution is to limit access to trusted users.

## References

http://www.zerodayinitiative.com/advisories/ZDI-09-081/

## Limitations

Exploit works on HP Power Manager 4.2.7. Windows patch KB933729 (rpct4.dll version 5.2.3790.4115) must be installed.

---

## HP Universal CMDB Server Axis2 default password

**Severity:** Unsuccessful Exploit          **CVE:**  CVE-2010-0219

## Resolution

Change the password for the admin account in the axis2.xml file, which is found in the \hp\UCMDB\UCMDBServer\deploy\axis2\WEB-INF\conf\ folder.

## References

http://www.securityfocus.com/archive/1/515494

## Limitations

Exploit works on HP Universal CMDB Server 9.0.

There may be a delay before the exploit succeeds.

---

## IBM Rational Quality Manager and Test Lab Manager Policy Bypass

**Severity:** Unsuccessful Exploit          **CVE:**  CVE-2010-4094

## Resolution

Download the fix for IBM Rational Quality Manager 2.0.1 from IBM.

## References

http://www.zerodayinitiative.com/advisories/ZDI-10-214/

## Limitations

Exploit works on IBM Rational Quality Manager 2.0.1 on Microsoft Windows Server 2003 and Windows Server 2008.

It may take longer than usual to establish the connection after successful exploitation because it takes time for the affected server to deploy the malicious WAR file.

---

## Internet Explorer iepeers.dll use-after-free vulnerability

**Severity:** Unsuccessful Exploit          **CVE:**  CVE-2010-0806

## Resolution

Apply the update referenced in MS10-018.

## References

http://www.kb.cert.org/vuls/id/744549

## Limitations

Exploit works on Internet Explorer 7 and requires a user to load the exploit page.

---

## Internet Explorer IFRAME buffer overflow

**Severity:** Unsuccessful Exploit                    **CVE:**  CVE-2004-1050

## Resolution

Apply the update referenced in Microsoft Security Bulletin 04-040 or a later cumulative Internet Explorer update.

## References

http://www.kb.cert.org/vuls/id/842160

## Limitations

Exploit works on Internet Explorer 6. Exploitation requires a user to load the exploit into Internet Explorer.

---

## InterSystems Cache HTTP Stack Buffer Overflow

**Severity:** Unsuccessful Exploit

## Resolution

Upgrade or apply a patch when it becomes available.

## References

None available at this time.

## Limitations

None.

---

## RedHat JBoss Enterprise Application Platform JMX Console Authentication Bypass

**Severity:** Unsuccessful Exploit                    **CVE:**  CVE-2010-0738

## Resolution

JBoss Enterprise Application Platform should be upgraded to 4.3 CP08, 4.2 CP09, or higher.

To secure the JMX Console, use the advanced installer options to configure JBoss to only allow authenticated administrative access.

**References**

http://secunia.com/advisories/39563/

**Limitations**

Exploit works on Red Hat JBoss Enterprise Application Platform 4.2.0.CP08.

The JMX Console service must be accessible remotely. By default, it is only accessible locally.

## JRun mod_jrun WriteToLog buffer overflow

**Severity:** Unsuccessful Exploit          **CVE:** CVE-2004-0646

**Resolution**

Apply the patch referenced in Macromedia Security Bulletin 04-08.

**References**

http://www.idefense.com/intelligence/vulnerabilities/display.php?id=145&type=vulnerabilities

**Limitations**

Exploit works on JRun 4 SP1a with verbose logging enabled.

## Microsoft WMI Administrative Tools ActiveX Control AddContextRef vulnerability

**Severity:** Unsuccessful Exploit          **CVE:** CVE-2010-3973

**Resolution**

Set the kill bit for Class ID 2745E5F5-D234-11D0-847A-00C04FD7BB08 as described in Microsoft Knowledge Base Article 240797.

**References**

http://www.kb.cert.org/vuls/id/725596

**Limitations**

Exploit works on Microsoft WMI Administrative Tools 1.1 on Windows XP SP3 and Vista SP2, and requires a user to open the exploit page in Internet Explorer 6 or 7.

## Microsoft Windows Movie Maker IsValidWMToolsStream buffer overflow

**Severity:** Unsuccessful Exploit          **CVE:** CVE-2010-0265

**Resolution**

Apply the update referenced in Microsoft Security Bulletin 10-016.

**References**

http://seclists.org/fulldisclosure/2010/Mar/173

## Limitations

Exploit works on Windows Movie Maker 2.1 and requires a user to open the exploit file.

## Nagios statuswml.cgi Command Injection

**Severity:** Unsuccessful Exploit **CVE:** CVE-2009-2288

### Resolution

Upgrade to Nagios 3.1.1 or later.

### References

http://secunia.com/advisories/35543/

### Limitations

Exploit works on Nagios 2.11.
Valid Nagios user credentials must be provided.

## Windows NetDDE buffer overflow

**Severity:** Unsuccessful Exploit **CVE:** CVE-2004-0206

### Resolution

Disable the NetDDE service or install the patch referenced in Microsoft Security Bulletin 04-031.

### References

http://www.microsoft.com/technet/security/Bulletin/MS04-031.mspx

## Novell Client NetIdentity Agent XTIERRPCPIPE pointer dereference vulnerability

**Severity:** Unsuccessful Exploit **CVE:** CVE-2009-1350

### Resolution

Apply the Novell NetIdentity 1.2.4 patch.

### References

http://www.zerodayinitiative.com/advisories/ZDI-09-016/

### Limitations

Exploit works on Novell NetIdentity Agent 1.2.3 and requires a valid Windows login and password.

The Crypt::DES, Digest::MD4, and Digest::MD5 packages are required for performing Windows authentication. These packages are available from http://cpan.org/modules/by-module/.

## Novell Client nwspool.dll buffer overflow

**Severity:** Unsuccessful Exploit **CVE:** CVE-2006-5854

## Resolution

Apply `491psp3_nwspool.exe`. Patches are available from Novell.

## References

http://www.securityfocus.com/archive/1/453012
http://www.novell.com/support/search.do?cmd=displayKC&externalId=3125538&sliceId=SAL_Public

## Limitations

Exploit works on Novell Client 4.91 SP3 on Windows 2000.

---

## Novell Client 4.91 SP4 nwspool.dll buffer overflow

**Severity:** Unsuccessful Exploit          **CVE:** CVE-2007-6701

### Resolution

Install the Novell Client 4.91 Post-SP4 nwspool.dll.

### References

http://www.zerodayinitiative.com/advisories/ZDI-07-045.html

### Limitations

Exploit works on Novell Client for Windows 4.91 SP4.

For Windows Server 2003 targets, a shared printer must be configured before running the exploit, and valid user credentials with Administrator privileges must be provided.

The Crypt::DES, Digest::MD4, and Digest::MD5 packages are required for performing Windows authentication, which is a requirement for successful exploitation on Windows Server 2003. These packages are available from http://cpan.org/modules/by-module/.

---

## Novell iManager EnteredClassName buffer overflow

**Severity:** Unsuccessful Exploit          **CVE:** CVE-2010-1929

### Resolution

Upgrade to Novell iManager version 2.7.3 ftf4 or 2.7.4.

### References

http://www.vupen.com/english/advisories/2010/1575

### Limitations

Exploit works on Novell iManager 2.7.3 and requires a valid Novell iManager login, password, and tree name.

---

## Novell iManager getMultiPartParameters file upload vulnerability

**Severity:** Unsuccessful Exploit

**Resolution**

Apply the patch referenced in Novell document 7006515.

**References**

http://www.zerodayinitiative.com/advisories/ZDI-10-190/

**Limitations**

Exploit works on Novell iManager 2.7.3.

If successful, this exploit creates a web application called exploit.war on the target.

Because it takes time for the target to deploy the web application sent by the exploit, there may be a delay before the exploit succeeds.

## HP OpenView Network Node Manager getnnmdata.exe CGI Hostname buffer overflow

**Severity:** Unsuccessful Exploit          **CVE:**   CVE-2010-1555

**Resolution**

Apply the fix referenced in HPSBMA02527 SSRT010098.

**References**

http://zerodayinitiative.com/advisories/ZDI-10-086/

**Limitations**

Exploit works on HP OpenView Network Node Manager 7.53.

On Windows Server 2003, Read and Execute privileges on the file '%windir%\system32\cmd.exe' must be granted to the Internet Guest Account "IUSR_<computername>" for the exploit to work properly.

## HP OpenView NNM getnnmdata.exe CGI ICount Parameter Buffer Overflow

**Severity:** Unsuccessful Exploit          **CVE:**   CVE-2010-1554

**Resolution**

Apply the fix referenced in HPSBMA02527 SSRT010098.

**References**

http://www.zerodayinitiative.com/advisories/ZDI-10-085/

**Limitations**

Exploit works on HP OpenView Network Node Manager 7.53.

On Windows Server 2003, Read and Execute privileges on the file '%windir%\system32\cmd.exe' must be granted to the Internet Guest Account "IUSR_<computername>" for the exploit to work properly.

## HP OpenView Network Node Manager getnnmdata.exe CGI MaxAge buffer overflow

**Severity:** Unsuccessful Exploit          **CVE:**   CVE-2010-1553

### Resolution

Apply the fix referenced in HPSBMA02527 SSRT010098.

### References

http://www.zerodayinitiative.com/advisories/ZDI-10-084/

### Limitations

Exploit works on HP OpenView Network Node Manager 7.53.

On Windows Server 2003, Read and Execute privileges on the file '%windir%\system32\cmd.exe' must be granted to the Internet Guest Account "IUSR_<computername>" for the exploit to work properly.

---

## HP OpenView Network Node Manager malformed displayWidth option to jovgraph.exe

**Severity:** Unsuccessful Exploit          **CVE:**   CVE-2011-0261

### Resolution

Apply the appropriate patch.

### References

http://www.zerodayinitiative.com/advisories/ZDI-11-003/

### Limitations

Exploit works on HP OpenView Network Node Manager 7.53 on Windows Server 2003 with DEP AlwaysOff.

On Windows Server 2003, read and execute privileges on the file `%windir%\system32\cmd.exe` must be granted to the Internet Guest Account `IUSR_<computername>` for the exploit to work properly. Note that users in the `Users` and `Power Users` groups do not have such privileges, but users in the `Administrators` and `TelnetClients` groups do.

---

## HP OpenView Network Node Manager nnmRptConfig.exe CGI Template Buffer Overflow

**Severity:** Unsuccessful Exploit          **CVE:**   CVE-2009-3848

### Resolution

Apply the appropriate patch.

### References

http://secunia.com/advisories/37665/

### Limitations

Exploit works on HP OpenView Network Node Manager 7.53 with the patch NNM_01200 on Windows Server 2003.

On Windows Server 2003, read and execute privileges on the file `%windir%\system32\cmd.exe` must be granted to the Internet Guest Account `IUSR_<computername>` for the exploit to work properly. Note that users in the `Users` and `Power Users` groups do not have such privileges, but users in the `Administrators` and `TelnetClients` groups do.

## HP OpenView Network Node Manager nnmRptConfig.exe nameParams text1 Buffer Overflow

**Severity:** Unsuccessful Exploit          **CVE:** CVE-2011-0268

### Resolution

Apply the appropriate patch.

### References

http://www.zerodayinitiative.com/advisories/ZDI-11-010/

### Limitations

Exploit works on HP OpenView Network Node Manager 7.53 with security update KB925902 on Windows Server 2003.

On Windows Server 2003, read and execute privileges on the file `%windir%\system32\cmd.exe` must be granted to the Internet Guest Account `IUSR_<computername>` for the exploit to work properly. Note that users in the `Users` and `Power Users` groups do not have such privileges, but users in the `Administrators` and `TelnetClients` groups do.

## HP OpenView Network Node Manager nnmRptConfig.exe schd_select1 Remote Code Execution

**Severity:** Unsuccessful Exploit          **CVE:** CVE-2011-0269

### Resolution

Apply the appropriate patch.

### References

http://www.zerodayinitiative.com/advisories/ZDI-11-011/

### Limitations

Exploit works on HP OpenView Network Node Manager 7.53 with security update KB925902 on Windows Server 2003.

On Windows Server 2003, read and execute privileges on the file `%windir%\system32\cmd.exe` must be granted to the Internet Guest Account `IUSR_<computername>` for the exploit to work properly. Note that users in the `Users` and `Power Users` groups do not have such privileges, but users in the `Administrators` and `TelnetClients` groups do.

## HP OpenView Network Node Manager OpenView5.exe buffer overflow

**Severity:** Unsuccessful Exploit          **CVE:** CVE-2008-0067

**Resolution**

Apply one of the patches referenced in HPSBMA02400 SSRT080144.

**References**

http://secunia.com/secunia_research/2008-13/

**Limitations**

Exploit works on HP OpenView Network Node Manager 7.53 on Windows 2000.

---

## HP OpenView Network Node Manager ovalarm.exe Accept-Language buffer overflow

**Severity:** Unsuccessful Exploit  **CVE:** CVE-2009-4179

**Resolution**

See HPSBMA02483 SSRT090257 rev.2 for patch information.

**References**

http://archives.neohapsis.com/archives/bugtraq/2009-12/0164.html

**Limitations**

Exploit works on HP OpenView Network Node Manager 7.53 with the patch NNM_01200 on Windows Server 2003 SP2 with the patch KB933729.

Read and Execute privileges on the file %windir%\system32\cmd.exe must be granted to the Internet Guest Account "IUSR_<computername>" for the exploit to work properly.

---

## HP OpenView Network Node Manager ovlogin.exe buffer overflow

**Severity:** Unsuccessful Exploit  **CVE:** CVE-2007-6204

**Resolution**

Apply one of the patches referenced in HPSBMA02281 SSRT061261.

**References**

http://www.zerodayinitiative.com/advisories/ZDI-07-071.html

**Limitations**

Exploit works on HP OpenView Network Node Manager 6.41 on Windows 2000.

---

## HP OpenView Network Node Manager ovwebsnmpsrv.exe buffer overflow via jovgraph.exe

**Severity:** Unsuccessful Exploit  **CVE:** CVE-2009-4181

**Resolution**

Apply the fix referenced in HPSBMA02483 SSRT090257.

## References

http://archives.neohapsis.com/archives/bugtraq/2009-12/0166.html

## Limitations

Exploit works on HP OpenView Network Node Manager 7.53 with the patch NNM_01200.

---

## HP OpenView Network Node Manager snmpviewer.exe CGI Stack Buffer Overflow

**Severity:** Unsuccessful Exploit          **CVE:** CVE-2010-1552

### Resolution

Apply the patches referenced in HP Security Bulletin HPSBMA02527 SSRT010098.

### References

http://secunia.com/advisories/39757/

### Limitations

Exploit works on HP OpenView Network Node Manager 7.53.

On Windows Server 2003, `Read` and `Execute` privileges on the file `%windir%\system32\cmd.exe` must be granted to the Internet Guest Account `IUSR_<computername>` for the exploit to work properly. Note that users in the groups `Users` and `Power Users` don't have those privileges, but users in the groups `Administrators` and `TelnetClients` do.

---

## HP OpenView Network Node Manager Toolbar.exe CGI buffer overflow

**Severity:** Unsuccessful Exploit          **CVE:** CVE-2008-0067

### Resolution

Apply a fix when available, or restrict access to the `Toolbar.exe` CGI program.

### References

http://secunia.com/secunia_research/2008-13/

### Limitations

Exploit works on HP OpenView Network Node Manager 7.5 on Windows 2000.

---

## Serv-U Web Client session cookie handling buffer overflow

**Severity:** Unsuccessful Exploit

### Resolution

Upgrade to a Serv-U version higher than 9.0.0.5 when it becomes available. Until an update is available, disable the Web Client Service and only use the Serv-U FTP/SFTP components.

### References

http://www.rangos.de/ServU-ADV.txt

**Limitations**

Exploit works on Rhino Software Serv-U 9.0.0.5. Windows patch KB933729 (rpcrt4.dll version 5.2.3790.4115) must be installed. The exploit may need to be executed multiple times to trigger the vulnerability.

---

**Windows password weakness**

**Severity:** Unsuccessful Exploit    **CVE:**   CVE-1999-0503

**Resolution**

Protect all accounts with a password that cannot be guessed. Require users to choose passwords which are eight charactes long, including numeric and non-alphanumeric characters, and which are not based on the login name or any other personal information about the user.

**References**

http://www.securityfocus.com/infocus/1537

**Limitations**

This exploit performs password guessing, not cracking. Therefore, a full dictionary attack will take a long time due to network latency. Guessing more than two passwords in rapid succession against user accounts will lock out accounts on systems with typical lockout policies. Successful password guesses do not result in a SAINTexploit connection unless the user has rights to a shared drive.

---

**Snort Back Orifice Pre-Processor buffer overflow**

**Severity:** Unsuccessful Exploit    **CVE:**   CVE-2005-3252

**Resolution**

Upgrade to Snort 2.4.3 or higher.

**References**

http://www.kb.cert.org/vuls/id/175500

**Limitations**

Exploit works on Snort 2.4.2 on Windows and Red Hat 8.

---

**Snort DCE/RPC preprocessor buffer overflow**

**Severity:** Unsuccessful Exploit    **CVE:**   CVE-2006-5276

**Resolution**

Upgrade to Snort 2.6.1.3 or higher.

**References**

http://www.us-cert.gov/cas/techalerts/TA07-050A.html

http://www.snort.org/docs/advisory-2007-02-19.html

**Limitations**

Exploit works on Snort 2.6.1.1 on Windows and Snort 2.6.1.2 on Red Hat 8, and requires port 445/TCP to be open on the target.

## Apache Struts2 XWork ParameterInterceptor security bypass

**Severity:** Unsuccessful Exploit                    **CVE:** CVE-2010-1870

**Resolution**

Upgrade to Apache Struts 2.2 or higher when available.

**References**

http://blog.o0o.nu/2010/07/cve-2010-1870-struts2xwork-remote.html

**Limitations**

Exploit works on Apache Struts 2.1.8.1. The specified share must be accessible by the target.

Before the exploit can succeed, exploit.exe must be placed on the specified share. Use the Download Connection or E-mail Attachment Execution exploit tool to obtain exploit.exe, using the same shell port as used with this exploit. Due to this requirement, this exploit must be run individually and is not included during an automated penetration test.

## Symantec Alert Management System Intel Alert Handler command execution

**Severity:** Unsuccessful Exploit

**Resolution**

Apply an update when available. If an update is not available, disable the Alert Handler service.

**References**

http://www.securityfocus.com/archive/1/512635

**Limitations**

Exploit works on Symantec System Center 10.1.8.8000. The specified share must be accessible by the target.

Before the exploit can succeed, exploit.exe must be placed on the specified share. Use the Download Connection or E-mail Attachment Execution exploit tool to obtain exploit.exe, using the same shell port as used with this exploit. Due to this requirement, this exploit must be run individually and is not included during an automated penetration test.

## TikiWiki file upload vulnerability (jhot.php)

**Severity:** Unsuccessful Exploit                    **CVE:** CVE-2006-4602

**Resolution**

Upgrade to TikiWiki 1.9.5 or higher.

## Trend Micro OfficeScan cgiRecvFile.exe ComputerName buffer overflow

**Severity:** Unsuccessful Exploit       **CVE:** CVE-2008-2437

### Resolution

Apply the appropriate patch.

### References

http://secunia.com/secunia_research/2008-35/

### Limitations

Exploit works on Trend Micro OfficeScan 7.3 Patch4.

Due to the nature of the vulnerability, the exploit is not 100% reliable on Windows Server 2003 targets with DEP enabled.

## Trend Micro OfficeScan Policy Server CGI buffer overflow

**Severity:** Unsuccessful Exploit       **CVE:** CVE-2008-1365

### Resolution

Restrict access to the OfficeScan HTTP port.

### References

http://secunia.com/advisories/29124/

### Limitations

Exploit works on Trend Micro OfficeScan Corporate Edition 7.3.

## TWiki revision control shell command injection

**Severity:** Unsuccessful Exploit       **CVE:** CVE-2005-2877

### Resolution

Apply the patch referenced in CIAC Bulletin P-307.

### References

http://archives.neohapsis.com/archives/bugtraq/2005-09/0154.html

## TWiki Search.pm shell command injection

**Severity:** Unsuccessful Exploit       **CVE:** CVE-2004-1037

**Resolution**

Apply the update referenced in CIAC Bulletin P-039.

**References**

http://archives.neohapsis.com/archives/bugtraq/2004-11/0181.html

## Windows LSASS buffer overflow

**Severity:** Unsuccessful Exploit      **CVE:** CVE-2003-0533

**Resolution**

Apply the patch referenced in Microsoft Security Bulletin 04-011.

**References**

http://www.kb.cert.org/vuls/id/753212

**Limitations**

This exploit may cause the target system to crash.

## Windows Plug and Play buffer overflow

**Severity:** Unsuccessful Exploit      **CVE:** CVE-2005-1983

**Resolution**

Apply the patch referenced in Microsoft Security Bulletin 05-047.

**References**

http://www.microsoft.com/technet/security/bulletin/MS05-039.mspx

**Limitations**

Remote, uncredentialed command execution is not possible on Windows XP or Windows Server 2003.

Successful exploitation may cause the target to reboot after disconnection.

## Windows RPC DCOM interface buffer overflow

**Severity:** Unsuccessful Exploit      **CVE:** CVE-2003-0352

**Resolution**

Install the patch referenced in Microsoft Security Bulletin 03-026.

**References**

http://www.cert.org/advisories/CA-2003-16.html

**Limitations**

> This exploit may cause the target system to crash.

## Windows RRAS memory corruption vulnerability

**Severity:** Unsuccessful Exploit          **CVE:**   CVE-2006-2370

### Resolution

Apply the patch referenced in Microsoft Security Bulletin 06-025.

### References

http://www.kb.cert.org/vuls/id/631516

### Limitations

The Remote Access Connection Manager service must be running in order for this exploit to succeed.

On Windows 2000, the Routing and Remote Access service must also be running and configured, and valid Windows login credentials are required. (Credentials are not required on Windows XP.)

The Crypt::DES, Digest::MD4, and Digest::MD5 packages are required for performing Windows authentication, which is a requirement for successful exploitation on Windows 2000. These packages are available from http://cpan.org/modules/by-module/.

## Windows Server Service buffer overflow

**Severity:** Unsuccessful Exploit          **CVE:**   CVE-2006-3439

### Resolution

Apply the patch referenced in Microsoft Security Bulletin 06-040.

### References

http://www.microsoft.com/technet/security/bulletin/ms06-040.mspx

### Limitations

Exploit works on Windows 2000 and Windows XP SP1. Target computer may reboot after connection is closed.

## Windows Server Service buffer overflow MS08-067

**Severity:** Unsuccessful Exploit          **CVE:**   CVE-2008-4250

### Resolution

Apply the patch referenced in Microsoft Security Bulletin 08-067.

### References

http://www.microsoft.com/technet/security/bulletin/MS08-067.mspx

### Limitations

Due to the nature of this vulnerability, the success of the exploit depends on the contents of unused stack memory space, and therefore is not completely reliable.

## Windows Thumbnail View CreateSizedDIBSECTION buffer overflow

**Severity:** Unsuccessful Exploit        **CVE:** CVE-2010-3970

### Resolution

See Microsoft Security Advisory 2490606 for fix information or workarounds.

### References

http://www.kb.cert.org/vuls/id/106516

### Limitations

Exploit works on Windows Explorer 5.1 on Windows XP.

## Windows Workstation service NetpManageIPCConnect buffer overflow

**Severity:** Unsuccessful Exploit        **CVE:** CVE-2006-4691

### Resolution

Install the patch referenced in Microsoft Security Bulletin 06-070.

### References

http://www.kb.cert.org/vuls/id/778036
http://archives.neohapsis.com/archives/bugtraq/2006-11/0245.html

### Limitations

Exploit works on Windows 2000 Service Pack 4. The SAINTexploit host must be able to bind to ports 53 /UDP and 389/UDP.

Exploit requires the target to be configured to use the SAINTexploit host as its DNS server. Since this situation is unlikely to exist in the real world, this exploit is probably more useful as a proof of concept than a penetration test.

## Wireshark LWRES dissector buffer overflow

**Severity:** Unsuccessful Exploit        **CVE:** CVE-2010-0304

### Resolution

Upgrade to Wireshark 1.2.6 or higher.

### References

http://www.wireshark.org/security/wnpa-sec-2010-02.html

### Limitations

Exploit works on Wireshark 1.0.3. Wireshark must be configured to capture and analyze the malicious traffic in order for the exploit to succeed.

**1900/UDP**

**Severity:** Service

**SMB**

**Severity:** Service

**WWW (non-standard port 2869)**

**Severity:** Service

**epmap (135/TCP)**

**Severity:** Service

**isakmp (500/UDP)**

**Severity:** Service

**microsoft-ds (445/TCP)**

**Severity:** Service

**microsoft-ds (445/UDP)**

**Severity:** Service

**netbios-dgm (138/UDP)**

**Severity:** Service

**netbios-ns (137/UDP)**

**Severity:** Service

**ntp (123/UDP)**

**Severity:** Service

## 4.3 192.168.0.14

**IP Address:** 192.168.0.14
**Scan time:** May 05 14:14:52 2011

**Host type:** Windows Server 2003
**Netbios Name:** 2K3

**Windows RPC DCOM interface buffer overflow**

**Severity:** Remote Administrator                    **CVE:**   CVE-2003-0352

**Resolution**

Install the patch referenced in Microsoft Security Bulletin 03-026.

**References**

http://www.cert.org/advisories/CA-2003-16.html

**Limitations**

This exploit may cause the target system to crash.

## Computer Associates Alert Notification Server buffer overflow

**Severity:** Unsuccessful Exploit                    **CVE:** CVE-2007-3825

**Resolution**

Apply fix QO89817.

**References**

http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=561
http://supportconnectw.ca.com/public/antivirus/infodocs/caantivirus-secnotice.asp

**Limitations**

Exploit works on CA BrightStor ARCserve Backup 11.5 and requires a valid login and password.

The Crypt::DES, Digest::MD4, and Digest::MD5 packages are required for performing Windows authentication, which is a requirement for successful exploitation. These packages are available from http://cpan.org/modules/by-module/.

## Computer Associates Alert Notification Server opcode 23 buffer overflow

**Severity:** Unsuccessful Exploit                    **CVE:** CVE-2007-4620

**Resolution**

Apply one of the updates referenced in the Security Notice.

**References**

http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=679

**Limitations**

Exploit works on CA eTrust Antivirus r8 with patch QO89817. Valid Windows credentials are required in order for this exploit to succeed.

## HP Data Protector Manager MMD Service Stack Buffer Overflow

**Severity:** Unsuccessful Exploit

**Resolution**

Apply a patch when it becomes available.

**References**

http://secunia.com/advisories/41735

**Limitations**

Exploit works on HP Data Protector Media Operations 6.11.

The Media Management Daemon service uses a dynamically assigned TCP port in the range 1024 to 65535.

## Windows NetDDE buffer overflow

| | |
|---|---|
| **Severity:** Unsuccessful Exploit | **CVE:** CVE-2004-0206 |

**Resolution**

Disable the NetDDE service or install the patch referenced in Microsoft Security Bulletin 04-031.

**References**

http://www.microsoft.com/technet/security/Bulletin/MS04-031.mspx

## Novell Client NetIdentity Agent XTIERRPCPIPE pointer dereference vulnerability

| | |
|---|---|
| **Severity:** Unsuccessful Exploit | **CVE:** CVE-2009-1350 |

**Resolution**

Apply the Novell NetIdentity 1.2.4 patch.

**References**

http://www.zerodayinitiative.com/advisories/ZDI-09-016/

**Limitations**

Exploit works on Novell NetIdentity Agent 1.2.3 and requires a valid Windows login and password.

The Crypt::DES, Digest::MD4, and Digest::MD5 packages are required for performing Windows authentication. These packages are available from http://cpan.org/modules/by-module/.

## Novell Client nwspool.dll buffer overflow

| | |
|---|---|
| **Severity:** Unsuccessful Exploit | **CVE:** CVE-2006-5854 |

**Resolution**

Apply `491psp3_nwspool.exe`. Patches are available from Novell.

**References**

http://www.securityfocus.com/archive/1/453012
http://www.novell.com/support/search.do?cmd=displayKC&externalId=3125538&sliceId=SAL_Public

**Limitations**

Exploit works on Novell Client 4.91 SP3 on Windows 2000.

## Novell Client nwspool.dll EnumPrinters buffer overflow

| | |
|---|---|
| **Severity:** Unsuccessful Exploit | **CVE:** CVE-2008-0639 |

## Resolution

Apply Novell Client 4.91 Post-SP2/3/4 nwspool.dll 2.

## References

http://www.zerodayinitiative.com/advisories/ZDI-08-005.html

## Limitations

Exploit works on Novell Client for Windows 4.91 SP4 with the 4.91 Post-SP2/3/4 nwspool.dll 1 patch.

In order for the exploit to succeed against Windows Server 2003 targets, a shared printer must be configured, the login and password of an account with administrator privileges must be provided, and the Crypt::DES, Digest::MD4, and Digest::MD5 PERL modules must be installed. These modules are available from http://cpan.org/modules/by-module/.

## Novell Client 4.91 SP4 nwspool.dll buffer overflow

**Severity:** Unsuccessful Exploit          **CVE:**   CVE-2007-6701

## Resolution

Install the Novell Client 4.91 Post-SP4 nwspool.dll.

## References

http://www.zerodayinitiative.com/advisories/ZDI-07-045.html

## Limitations

Exploit works on Novell Client for Windows 4.91 SP4.

For Windows Server 2003 targets, a shared printer must be configured before running the exploit, and valid user credentials with Administrator privileges must be provided.

The Crypt::DES, Digest::MD4, and Digest::MD5 packages are required for performing Windows authentication, which is a requirement for successful exploitation on Windows Server 2003. These packages are available from http://cpan.org/modules/by-module/.

## Windows password weakness

**Severity:** Unsuccessful Exploit          **CVE:**   CVE-1999-0503

## Resolution

Protect all accounts with a password that cannot be guessed. Require users to choose passwords which are eight charactes long, including numeric and non-alphanumeric characters, and which are not based on the login name or any other personal information about the user.

## References

http://www.securityfocus.com/infocus/1537

## Limitations

This exploit performs password guessing, not cracking. Therefore, a full dictionary attack will take a long time due to network latency. Guessing more than two passwords in rapid succession against user accounts will lock out accounts on systems with typical lockout policies. Successful password guesses do not result in a SAINTexploit connection unless the user has rights to a shared drive.

## Snort Back Orifice Pre-Processor buffer overflow

**Severity:** Unsuccessful Exploit                    **CVE:**  CVE-2005-3252

### Resolution

Upgrade to Snort 2.4.3 or higher.

### References

http://www.kb.cert.org/vuls/id/175500

### Limitations

Exploit works on Snort 2.4.2 on Windows and Red Hat 8.

## Apache Struts2 XWork ParameterInterceptor security bypass

**Severity:** Unsuccessful Exploit                    **CVE:**  CVE-2010-1870

### Resolution

Upgrade to Apache Struts 2.2 or higher when available.

### References

http://blog.o0o.nu/2010/07/cve-2010-1870-struts2xwork-remote.html

### Limitations

Exploit works on Apache Struts 2.1.8.1. The specified share must be accessible by the target.

Before the exploit can succeed, exploit.exe must be placed on the specified share. Use the Download Connection or E-mail Attachment Execution exploit tool to obtain exploit.exe, using the same shell port as used with this exploit. Due to this requirement, this exploit must be run individually and is not included during an automated penetration test.

## Symantec Alert Management System Intel Alert Handler command execution

**Severity:** Unsuccessful Exploit

### Resolution

Apply an update when available. If an update is not available, disable the Alert Handler service.

### References

http://www.securityfocus.com/archive/1/512635

**Limitations**

Exploit works on Symantec System Center 10.1.8.8000. The specified share must be accessible by the target.

Before the exploit can succeed, exploit.exe must be placed on the specified share. Use the Download Connection or E-mail Attachment Execution exploit tool to obtain exploit.exe, using the same shell port as used with this exploit. Due to this requirement, this exploit must be run individually and is not included during an automated penetration test.

## Windows DNS server RPC management interface buffer overflow

**Severity:** Unsuccessful Exploit          **CVE:** CVE-2007-1748

**Resolution**

See Microsoft Security Advisory 935964 for information on available updates and workarounds.

**References**

http://www.us-cert.gov/cas/techalerts/TA07-103A.html

**Limitations**

Exploit works on Windows 2000 SP0 to SP4 and Windows Server 2003 SP1 and SP2.

## Windows Plug and Play buffer overflow

**Severity:** Unsuccessful Exploit          **CVE:** CVE-2005-1983

**Resolution**

Apply the patch referenced in Microsoft Security Bulletin 05-047.

**References**

http://www.microsoft.com/technet/security/bulletin/MS05-039.mspx

**Limitations**

Remote, uncredentialed command execution is not possible on Windows XP or Windows Server 2003.

Successful exploitation may cause the target to reboot after disconnection.

## Windows Server Service buffer overflow MS08-067

**Severity:** Unsuccessful Exploit          **CVE:** CVE-2008-4250

**Resolution**

Apply the patch referenced in Microsoft Security Bulletin 08-067.

**References**

http://www.microsoft.com/technet/security/bulletin/MS08-067.mspx

## Limitations

Due to the nature of this vulnerability, the success of the exploit depends on the contents of unused stack memory space, and therefore is not completely reliable.

## Windows Workstation service NetpManageIPCConnect buffer overflow

**Severity:** Unsuccessful Exploit          **CVE:**  CVE-2006-4691

### Resolution

Install the patch referenced in Microsoft Security Bulletin 06-070.

### References

http://www.kb.cert.org/vuls/id/778036
http://archives.neohapsis.com/archives/bugtraq/2006-11/0245.html

### Limitations

Exploit works on Windows 2000 Service Pack 4. The SAINTexploit host must be able to bind to ports 53 /UDP and 389/UDP.

Exploit requires the target to be configured to use the SAINTexploit host as its DNS server. Since this situation is unlikely to exist in the real world, this exploit is probably more useful as a proof of concept than a penetration test.

## 1025/TCP
**Severity:** Service

## 1026/TCP
**Severity:** Service

## 1028/UDP
**Severity:** Service

## SMB
**Severity:** Service

## epmap (135/TCP)
**Severity:** Service

## isakmp (500/UDP)
**Severity:** Service

## microsoft-ds (445/TCP)
**Severity:** Service

## microsoft-ds (445/UDP)
**Severity:** Service

## netbios-dgm (138/UDP)
**Severity:** Service

## netbios-ns (137/UDP)
**Severity:** Service

## ntp (123/UDP)
**Severity:** Service

Scan Session: saint-data; Scan Policy: heavy; Scan Data Set: 7 May 2011 12:35