

Table of Contents

[Product Focus](#)

[This Week in Review](#)

[Top Security News Stories this Week](#)

[New Vulnerabilities Tested in SecureScout](#)

[New Vulnerabilities found this Week](#)

Product Focus

[ASN.1 Vulnerability Scanner](#) - The S4 ASN.1 Vulnerability Scanner is a free utility made by SecureScout that will scan up to 256 IP addresses at once to assess if any are vulnerable to the MS04-007 that could allow remote code execution.

Download Here:

<http://www.netvigilance.com/productdownloads?productname=asn.1vulnerabilityscanner>

This Week in Review

Mobile malware is coming. Beware when surfing for costumes. ID theft prevention plan to be required. Microsoft releases emergency patch. SecureScout emergency packages will be released over the weekend.

Enjoy reading & Stay safe.

Call or email netVigilance to get an update on SecureScout.

(503) 524 5758 or sales@netvigilance.com

Top Security News Stories this Week

• Mobile phone malware in our future?

Last week, a new report (PDF) on emerging threats from the Georgia Tech Information Security Center mentioned, among other predictions, that botnets were likely to hit mobile phones sometime in the next year. On Tuesday, I spoke with VeriSign CTO Ken Silva about that possibility and why it might happen within the coming year.

Silva said the mobile phone market is changing. Today's mobile phones don't just make phone calls, they stream video and support content. "Most consumers did not care about a smartphone until Windows Mobile, the Apple iPhone, and now Google Android came along. Now more and more consumers want smartphones. Kids want them; it's a cool phone to have."

Another compelling reason to think malware is coming soon to your smartphone is more bandwidth. Because of the streaming media options, this year's phones process data much faster than last year's models.

Full Story :

http://news.cnet.com/8301-10789_3-10071982-57.html?part=rss&tag=feed&subj=DefenseinDepth

• **Compromised Halloween websites passing along rogue software**

An internet search using the keywords "halloween costumes" may turn up a number of legitimate sites that have been compromised, and users might end up with rogue anti-virus software on their machine.

The Halloween attack uses search engine optimization manipulation to distribute the campaigns, according to a Wednesday TrendLabsblog post.

That way, when an unsuspecting web user searches those terms, the legitimate but compromised website will return a high ranking and he or she will be more likely to visit there.

SC Magazine

Full Story :

<http://www.scmagazineus.com/Compromised-Halloween-websites-passing-along-rogue-software/article/119809/>

• **FTC extends \"Red Flags Rules\" enforcement six months**

The Federal Trade Commission is extending the deadline for enforcement of the identity theft prevention "Red Flags Rules" until May 1.

The rules require that creditors and financial institutions create and implement an ID theft prevention program.

"There seems to be a lot of feedback from people saying that there's no way we can meet this deadline," Edward Goodman, general counsel and chief privacy officer for vendor Identity Theft 911, told SCMagazineUS.com Thursday.

SC Magazine

Full Story :

<http://www.scmagazineus.com/FTC-extends-Red-Flags-Rules-enforcement-six-months/article/119866/>

• **Separate proofs-of-concept released after rushed Windows fix**

Researchers have published separate proof-of-concept exploits that take advantage of the Windows vulnerability for which Microsoft rushed a patch on Thursday.

The Windows Server service flaw, addressed on Thursday when Microsoft pushed out a rare, out-of-cycle fix, can be exploited by sending malicious Remote Procedure Calls (RPCs) to vulnerable systems. Microsoft said it was aware of limited attacks targeting the bug, which, if not patched quickly enough, could have resulted in a major worm attack.

"This is exactly the kind of bug that triggered the big RPC worms of old," said Bas Alberts, a senior researcher at Immunity, a Miami-based security consultancy, referring to attacks such as Blaster and Code Red.

SC Magazine

Full Story :

<http://www.scmagazineus.com/Separate-proofs-of-concept-released-after-rushed-Windows-fix/article/119925/>

New Vulnerabilities Tested in SecureScout

• **14062 Samba allows local users to modify the membership of Unix groups Vulnerability**

Samba 3.2.0 uses weak permissions (0666) for the (1) group_mapping.tdb and (2) group_mapping.ldb files, which allows local users to modify the membership of Unix groups.

Samba version 3.2.3 fixes the issue.

Test Case Impact: **Gather Info** Vulnerability Impact: **Attack** Risk: **Low**

References:

* MLIST: [oss-security] 20080826 CVE Request (samba)

<http://www.openwall.com/lists/oss-security/2008/08/26/2>

* CONFIRM:

<http://bugs.debian.org/cgi-bin/bugreport.cgi?bug=496073>

* CONFIRM:

<http://samba.org/samba/security/CVE-2008-3789.html>

* BID: 30837
<http://www.securityfocus.com/bid/30837>
* SECTRACK: 1020770
<http://www.securitytracker.com/id?1020770>
* SECUNIA: 31601
<http://secunia.com/advisories/31601>
* XF: samba-groupmapping-security-bypass(44678)
<http://xforce.iss.net/xforce/xfdb/44678>

CVE Reference:

CVE-2008-3789 (cve.mitre.org, nvd.nist.gov)

• **18157 HIS Command Execution Vulnerability (MS08-059/956695) (Remote File Checking)**

A remote code execution vulnerability exists in the SNA Remote Procedure Call (RPC) service for Host Integration Server. An attacker could exploit the vulnerability by constructing a specially crafted RPC request. The vulnerability could allow remote code execution. An attacker who successfully exploited this vulnerability could take complete control of an affected system.

Test Case Impact: **Gather Info** Vulnerability Impact: **Attack** Risk: **High**

References:

* MS: MS08-059
<http://www.microsoft.com/technet/security/Bulletin/MS08-059.msp>
* BID: Microsoft Host Integration Server RPC Remote Command Execution Vulnerability
<http://www.securityfocus.com/bid/31620>
* FRSIRT: FrSIRT/ADV-2008-2810
<http://www.frsirt.com/english/advisories/2008/2810>
* SECTRACK: 1021043
<http://www.securitytracker.com/id?1021043>
* SECUNIA: 32233
<http://secunia.com/advisories/32233>

CVE Reference:

CVE-2008-3466 (cve.mitre.org, nvd.nist.gov)

• **18161 AFD Kernel Overwrite Vulnerability (MS08-066/956803) (Remote File Checking)**

An elevation of privilege vulnerability exists in the Ancillary Function Driver (afd.sys) due to Windows improperly validating input passed from user mode to the kernel. The vulnerability could allow an attacker to run code with elevated privileges. A local attacker who successfully exploited this vulnerability could execute arbitrary code and take complete control of an affected system. The attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

Test Case Impact: **Gather Info** Vulnerability Impact: **Attack / Gain Root** Risk: **High**

References:

* BUGTRAQ: 20081015 Exploit for MS08-066 - AFD.sys kernel memory overwrite.
<http://www.securityfocus.com/archive/1/archive/1/497375/100/0/threaded>
* MILWORM: 6757
<http://www.milw0rm.com/exploits/6757>
* MISC:
<http://blogs.technet.com/swi/archive/2008/10/14/ms08-066-how-to-correctly-validate-and-capture-user-mode-data.aspx>
* MS: MS08-066
<http://www.microsoft.com/technet/security/Bulletin/MS08-066.msp>
* BID: 31673
<http://www.securityfocus.com/bid/31673>
* FRSIRT: ADV-2008-2817
<http://www.frsirt.com/english/advisories/2008/2817>
* SECTRACK: 1021053
<http://www.securitytracker.com/id?1021053>
* SECUNIA: 32261
<http://secunia.com/advisories/32261>
* XF: win-afd-privilege-escalation(45578)
<http://xforce.iss.net/xforce/xfdb/45578>
* XF: win-ms08kb956803-update(45582)
<http://xforce.iss.net/xforce/xfdb/45582>

CVE Reference:

CVE-2008-3464 (cve.mitre.org, nvd.nist.gov)

• **18162 Windows Kernel Window Creation Vulnerability (MS08-061/954211) (Remote File Checking)**

An elevation of privilege vulnerability exists because the Windows kernel does not properly validate properties of a window passed during the new window creation process. An attacker who successfully exploited this vulnerability could run arbitrary code in kernel mode. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

Test Case Impact: **Gather Info** Vulnerability Impact: **Attack / Gain Root** Risk: **High**

References:

- * MS: MS08-061
<http://www.microsoft.com/technet/security/Bulletin/MS08-061.msp>
- * BID: 31651
<http://www.securityfocus.com/bid/31651>
- * FRSIRT: ADV-2008-2812
<http://www.frsirt.com/english/advisories/2008/2812>
- * SECTRACK: 1021046
<http://www.securitytracker.com/id?1021046>
- * SECUNIA: 32247
<http://secunia.com/advisories/32247>
- * XF: win-kernel-window-privilege-escalation(45541)
<http://xforce.iss.net/xforce/xfdb/45541>
- * XF: win-ms08kb954211-update(45544)
<http://xforce.iss.net/xforce/xfdb/45544>

CVE Reference:

CVE-2008-2250 (cve.mitre.org, nvd.nist.gov)

• **18163 Windows Kernel Unhandled Exception Vulnerability (MS08-061/954211) (Remote File Checking)**

An elevation of privilege vulnerability exists due to a possible "Double Free" condition in the Windows kernel. The vulnerability could allow an attacker to run code with elevated privileges. An attacker who successfully exploited this vulnerability could execute arbitrary code and take complete control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

Test Case Impact: **Gather Info** Vulnerability Impact: **Attack / Gain Root** Risk: **High**

References:

- * MS: MS08-061
<http://www.microsoft.com/technet/security/Bulletin/MS08-061.msp>
- * BID: 31653
<http://www.securityfocus.com/bid/31653>
- * FRSIRT: ADV-2008-2812
<http://www.frsirt.com/english/advisories/2008/2812>
- * SECTRACK: 1021046
<http://www.securitytracker.com/id?1021046>
- * SECUNIA: 32247
<http://secunia.com/advisories/32247>
- * XF: win-kernel-system-calls-privilege-escalation(45542)
<http://xforce.iss.net/xforce/xfdb/45542>
- * XF: win-ms08kb954211-update(45544)
<http://xforce.iss.net/xforce/xfdb/45544>

CVE Reference:

CVE-2008-2251 (cve.mitre.org, nvd.nist.gov)

• **18164 Windows Kernel Memory Corruption Vulnerability (MS08-061/954211) (Remote File Checking)**

An elevation of privilege vulnerability exists due to the Windows kernel improperly validating input passed from user mode to the kernel. The vulnerability could allow an attacker to run code with elevated privileges. An attacker who successfully exploited this vulnerability could execute arbitrary code and take complete control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

Test Case Impact: **Gather Info** Vulnerability Impact: **Attack / Gain Root** Risk: **High**

References:

* MS: MS08-061
<http://www.microsoft.com/technet/security/Bulletin/MS08-061.msp>
* BID: 31652
<http://www.securityfocus.com/bid/31652>
* FRSIRT: ADV-2008-2812
<http://www.frsirt.com/english/advisories/2008/2812>
* SECTRACK: 1021046
<http://www.securitytracker.com/id?1021046>
* SECUNIA: 32247
<http://secunia.com/advisories/32247>
* XF: win-kernel-input-privilege-escalation(45543)
<http://xforce.iss.net/xforce/xfdb/45543>
* XF: win-ms08kb954211-update(45544)
<http://xforce.iss.net/xforce/xfdb/45544>

CVE Reference:

CVE-2008-2252 (cve.mitre.org, nvd.nist.gov)

• 18165 Integer Overflow in IPP Service Vulnerability (MS08-062/953155) (Remote File Checking)

A remote code execution vulnerability exists on Windows systems running Microsoft Internet Information Services (IIS) with the Windows Internet Printing service enabled. This issue could allow a remote, authenticated attacker to execute arbitrary code on an affected system.

Test Case Impact: **Gather Info** Vulnerability Impact: **Attack** Risk: **High**

References:

* MS: MS08-062
<http://www.microsoft.com/technet/security/Bulletin/MS08-062.msp>
* CERT-VN: VU#793233
<http://www.kb.cert.org/vuls/id/793233>
* BID: 31682
<http://www.securityfocus.com/bid/31682>
* FRSIRT: ADV-2008-2813
<http://www.frsirt.com/english/advisories/2008/2813>
* SECTRACK: 1021048
<http://www.securitytracker.com/id?1021048>
* SECUNIA: 32248
<http://secunia.com/advisories/32248>
* XF: win-ipp-service-code-execution(45545)
<http://xforce.iss.net/xforce/xfdb/45545>
* XF: win-ms08kb953155-update(45548)
<http://xforce.iss.net/xforce/xfdb/45548>

CVE Reference:

CVE-2008-1446 (cve.mitre.org, nvd.nist.gov)

• 18166 SMB Buffer Underflow Vulnerability (MS08-063/957095) (Remote File Checking)

A remote code execution vulnerability exists in the way that Microsoft Server Message Block (SMB) Protocol handles specially crafted file names. An attempt to exploit the vulnerability would require authentication because the vulnerable function is only reachable when the share type is a disk, and by default, all disk shares require authentication. An attacker who successfully exploited this vulnerability could install programs; view, change, or delete data; or create new accounts with full user rights.

Test Case Impact: **Gather Info** Vulnerability Impact: **Attack** Risk: **High**

References:

* MS: MS08-063
<http://www.microsoft.com/technet/security/Bulletin/MS08-063.msp>
* BID: 31647
<http://www.securityfocus.com/bid/31647>
* FRSIRT: ADV-2008-2814
<http://www.frsirt.com/english/advisories/2008/2814>
* SECTRACK: 1021049
<http://www.securitytracker.com/id?1021049>
* SECUNIA: 32249
<http://secunia.com/advisories/32249>
* XF: win-ms08kb957095-update(45561)

<http://xforce.iss.net/xforce/xfdb/45561>

* XF: win-smb-filename-bu(45560)

<http://xforce.iss.net/xforce/xfdb/45560>

CVE Reference:

CVE-2008-4038 (cve.mitre.org, nvd.nist.gov)

• 18167 Virtual Address Descriptor Elevation of Privilege Vulnerability (MS08-064/956841) (Remote File Checking)

An elevation of privilege vulnerability exists in the way that Memory Manager handles memory allocation and Virtual Address Descriptors (VADs). The vulnerability could allow elevation of privilege if an authenticated attacker runs a specially crafted program on an affected system. An attacker who successfully exploited this vulnerability could gain elevation of privilege on an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full administrative rights.

Test Case Impact: **Gather Info** Vulnerability Impact: **Attack / Gain Root** Risk: **High**

References:

* MS: MS08-064

<http://www.microsoft.com/technet/security/Bulletin/MS08-064.mspx>

* BID: 31675

<http://www.securityfocus.com/bid/31675>

* FRSIRT: ADV-2008-2815

<http://www.frsirt.com/english/advisories/2008/2815>

* SECTRACK: 1021051

<http://www.securitytracker.com/id?1021051>

* SECUNIA: 32251

<http://secunia.com/advisories/32251>

* XF: win-ms08kb956841-update(45572)

<http://xforce.iss.net/xforce/xfdb/45572>

* XF: win-vad-privilege-escalation(45571)

<http://xforce.iss.net/xforce/xfdb/45571>

CVE Reference:

CVE-2008-4036 (cve.mitre.org, nvd.nist.gov)

• 18168 Message Queuing Service Remote Code Execution Vulnerability (MS08-065/951071) (Remote File Checking)

A remote code execution vulnerability exists in the Message Queuing Service due to a specific flaw in the parsing of an RPC request to the Message Queuing service.

An attacker could exploit the vulnerability by sending a specially crafted RPC request. A heap request can be controlled and later overflowed during an unchecked string copy operation. Successful exploitation of this issue could lead to full access to the affected system under the SYSTEM context. An attacker who successfully exploited this vulnerability could take complete control of an affected system.

Test Case Impact: **Gather Info** Vulnerability Impact: **Attack** Risk: **High**

References:

* MS: MS08-065

<http://www.microsoft.com/technet/security/Bulletin/MS08-065.mspx>

* FRSIRT: ADV-2008-2816

<http://www.frsirt.com/english/advisories/2008/2816>

* SECTRACK: 1021052

<http://www.securitytracker.com/id?1021052>

* SECUNIA: 32260

<http://secunia.com/advisories/32260>

* XF: win-ms08kb951071-update(45538)

<http://xforce.iss.net/xforce/xfdb/45538>

* XF: win-msmq-rpc-code-execution(45537)

<http://xforce.iss.net/xforce/xfdb/45537>

CVE Reference:

CVE-2008-3479 (cve.mitre.org, nvd.nist.gov)

New Vulnerabilities found this Week

• CVE-2008-4609 Microsoft CVSS 2.0 Score = 7.1

The TCP implementation in (1) Linux, (2) platforms based on BSD Unix, (3) Microsoft Windows, (4) Cisco products, and probably other operating systems allows remote attackers to cause a denial of service (connection queue exhaustion) via multiple vectors that manipulate information in the TCP state table, as demonstrated by sockstress. Please see also: <http://blog.robertlee.name/2008/10/more-detailed-response-to-gordons-post.html> and <http://www.curbrisk.com/security-blog/robert-e-lee-discusses-tcp-denial-service-vulnerability-sc-magazine.html>

Test Case Impact: Vulnerability Impact: Risk: **High**

References:

MISC: <https://www.cert.fi/haavoittuvuudet/2008/tcp-vulnerabilities.html>

MISC: <http://www.outpost24.com/news/news-2008-10-02.html>

CISCO: http://www.cisco.com/en/US/products/products_security_response09186a0080a15120.html

MISC: <http://searchsecurity.techtarget.com.au/articles/27154-TCP-is-fundamentally-borked>

MLIST: <http://lists.immunitysec.com/pipermail/dailydave/2008-October/005360.html>

MISC: <http://blog.robertlee.name/2008/10/conjecture-speculation.html>

CVE Reference: [CVE-2008-4609](#)

• CVE-2008-4609 Cisco CVSS 2.0 Score = 7.1

The TCP implementation in (1) Linux, (2) platforms based on BSD Unix, (3) Microsoft Windows, (4) Cisco products, and probably other operating systems allows remote attackers to cause a denial of service (connection queue exhaustion) via multiple vectors that manipulate information in the TCP state table, as demonstrated by sockstress. Please see also: <http://blog.robertlee.name/2008/10/more-detailed-response-to-gordons-post.html> and <http://www.curbrisk.com/security-blog/robert-e-lee-discusses-tcp-denial-service-vulnerability-sc-magazine.html>

Test Case Impact: Vulnerability Impact: Risk: **High**

References:

MISC: <https://www.cert.fi/haavoittuvuudet/2008/tcp-vulnerabilities.html>

MISC: <http://www.outpost24.com/news/news-2008-10-02.html>

CISCO: http://www.cisco.com/en/US/products/products_security_response09186a0080a15120.html

MISC: <http://searchsecurity.techtarget.com.au/articles/27154-TCP-is-fundamentally-borked>

MLIST: <http://lists.immunitysec.com/pipermail/dailydave/2008-October/005360.html>

MISC: <http://blog.robertlee.name/2008/10/conjecture-speculation.html>

CVE Reference: [CVE-2008-4609](#)

• CVE-2008-3831 Linux CVSS 2.0 Score = 4.7

The i915 driver in (1) drivers/char/drm/i915_dma.c in the Linux kernel 2.6.24 on Debian GNU/Linux and (2) sys/dev/pci/drm/i915_drv.c in OpenBSD does not restrict the DRM_I915_HWS_ADDR ioctl to the Direct Rendering Manager (DRM) master, which allows local users to cause a denial of service (memory corruption) via a crafted ioctl call, related to absence of the DRM_MASTER and DRM_ROOT_ONLY flags in the ioctl's configuration.

Test Case Impact: Vulnerability Impact: Risk: **Medium**

References:

BID: <http://www.securityfocus.com/bid/31792>

CONFIRM: http://www.openbsd.org/cgi-bin/cvsweb/src/sys/dev/pci/drm/i915_drv.c.diff?r1=1.7;r2=1.8

CONFIRM: http://www.openbsd.org/cgi-bin/cvsweb/src/sys/dev/pci/drm/i915_drv.c

DEBIAN: <http://www.debian.org/security/2008/dsa-1655>

SECTRAK: <http://securitytracker.com/id?1021065>

CONFIRM: http://security.debian.org/pool/updates/main/l/linux-2.6.24/linux-2.6.24_2.6.24-6~etchnhalf.6.diff.gz

MLIST: <http://archives.neohapsis.com/archives/openbsd/cvs/2008-10/0365.html>

CVE Reference: [CVE-2008-3831](#)

Vulnerability Resource

Check out this compendium of links and up-to-the minute information about network security issues. Their claim to be the 'security portal for information system security professionals' is well founded. <http://www.infosyssec.org/infosyssec/>

Thank You

Thanks for sifting through another great edition of the ScoutNews. We hope we captured a flavor for the week and gave you just enough information on newly found vulnerabilities to keep you up-to-date. To subscribe or unsubscribe, contact us at ScoutNews@netVigilance.com

About SecureScout

SecureScout is a leading vulnerability scanner and management tool developed and marketed worldwide by NexantiS Corporation.

SecureScout is a trademark of NexantiS Corporation.

netVigilance, Inc. is a partner of NexantiS and an authorized distributor of SecureScout.

For any inquiry about SecureScout by:

Customers in America and Northern Europe contact us at info@netVigilance.com

Customers in France, Italy, Spain, Portugal, Greece, Turkey, Eastern Europe, Middle East, Africa and Asia/Pacific, contact NexantiS at info-scanner@securescout.net