

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

[Request Tracker for Windows \(WinRT\) by SecureScout Free Edition \(no upgrade\) v3.4.5 beta2](#) - Download Free
WinRT v3.4.5 beta2 installer by filling our download form. Size: 34MB

Download Here:

http://www.netvigilance.com/productdownloads?productname=winrt_setup_3_4_5

This Week in Review

Some harsh words on a new buzz. Botnet growth exploding. Another look at security in an ever changing world. Better ROI with better security?

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

• Get Smashed, Not Mashed

September 1, 2008 (Computerworld) I hate to be the teetotaler at the mashup party, but someone has to take a sober look at the security implications of this emerging approach to business intelligence.

Think about that for a minute. Data from somewhere else running on your network? Even if the person who initiates the mashup believes the data comes from a trusted source, do you know if the originating systems meet your security standards? Are those systems at current patch levels? If your business works in a regulated environment, will such a mashup put you out of compliance?

Oh, and then there's JavaScript. Does the mashup your company is creating include JavaScript from outside your company?

Computerworld

Full Story :

http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=323888&source=rss_topic17

• Botnet spread skyrockets in summer

The number of computers infected with botnets has quadrupled during the last three months, according to data released by volunteer watchdog Shadowserver Foundation.

"This monitoring allows us to get a glimpse into the drones joining the party," he said.

"The surface area is getting larger, in terms of attack vectors, which means more compromised machines and a greater number of botnets," DiMino said.

SC Magazine

Full Story :

<http://www.scmagazineus.com/Botnet-spread-skyrockets-in-summer/article/116267/>

• Are you insecure about SOA security?

September 4, 2008 (CIO) Service-oriented architecture (SOA) creates tremendous opportunities for companies to integrate across departments, across systems and across enterprises. Integration can help simplify business processes, improve speed to market, allow companies to react quicker to changes in the business and share data and services.

SOA also allows companies to rejuvenate their legacy systems by abstracting certain business processes, services or data points without having to rip out and replace these systems. Companies can leverage their existing investments in their legacy systems while building new systems that seamlessly integrate with them.

Integration side effects The benefits I mentioned above come with great risks in the area of security, privacy and compliance. For services to integrate easily with other services both behind and outside of the firewall, they must be discoverable and easy to translate.

Computerworld

Full Story :

http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9114101&source=rss_topic1

• Security ROI: Fact or fiction?

September 4, 2008 (CSO) Return on investment, or ROI, is a big deal in business. Any business venture needs to demonstrate a positive return on investment, and a good one at that, in order to be viable.

It's a good idea in theory, but it's mostly bunk in practice.

But as anyone who has lived through a company's vicious end-of-year budget-slashing exercises knows, when you're trying to make your numbers, cutting costs is the same as increasing revenues. So while security can't produce ROI, loss prevention most certainly affects a company's bottom line.

Computerworld

Full Story :

http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9114021&source=rss_topic1

New Vulnerabilities Tested in SecureScout

• 18079 Winamp Multiple Vendor FLAC Library Multiple Integer Overflow Vulnerabilities (Remote File Checking)

Remote exploitation of multiple integer overflow vulnerabilities in libFLAC, as included with various vendor's software distributions, allows attackers to execute arbitrary code in the context of the currently logged in user.

These vulnerabilities specifically exist in the handling of malformed FLAC media files. In each case, an integer overflow can occur while calculating the amount of memory to allocate. As such, insufficient memory is allocated for the data that is subsequently read in from the file, and a heap based buffer overflow occurs.

The vulnerability is confirmed in version 5.x before 5.5.

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

References:

* IDEFENSE: 20071011 Multiple Vendor FLAC Library Multiple Integer Overflow Vulnerabilities

<http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=608>

* CONFIRM:

http://flac.sourceforge.net/changelog.html#flac_1_2_1

* CONFIRM:

http://bugzilla.redhat.com/show_bug.cgi?id=331991

* CONFIRM:

https://bugzilla.redhat.com/show_bug.cgi?id=332571

* CONFIRM:

<http://wiki.rpath.com/wiki/Advisories:rPSA-2007-0243>

* CONFIRM:

<https://issues.rpath.com/browse/RPL-1873>

* DEBIAN: DSA-1469

<http://www.debian.org/security/2008/dsa-1469>

* FEDORA: FEDORA-2007-2596

<https://www.redhat.com/archives/fedora-package-announce/2007-November/msg00035.html>

* GENTOO: GLSA-200711-15

<http://security.gentoo.org/glsa/glsa-200711-15.xml>

* MANDRIVA: MDKSA-2007:214

<http://www.mandriva.com/security/advisories?name=MDKSA-2007:214>

* REDHAT: RHSA-2007:0975

<http://www.redhat.com/support/errata/RHSA-2007-0975.html>

* SUSE: SUSE-SR:2007:022

<http://lists.opensuse.org/opensuse-security-announce/2007-10/msg00008.html>

* UBUNTU: USN-540-1

<http://www.ubuntu.com/usn/usn-540-1>

* BID: 26042

<http://www.securityfocus.com/bid/26042>

* FRSIRT: ADV-2007-3483

<http://www.frsirt.com/english/advisories/2007/3483>

* FRSIRT: ADV-2007-3484

<http://www.frsirt.com/english/advisories/2007/3484>

* FRSIRT: ADV-2007-4061

<http://www.frsirt.com/english/advisories/2007/4061>

* SECTRAK: 1018815

<http://securitytracker.com/id?1018815>

* SECUNIA: 27210

<http://secunia.com/advisories/27210>

* SECUNIA: 27223

<http://secunia.com/advisories/27223>

* SECUNIA: 27355

<http://secunia.com/advisories/27355>

* SECUNIA: 27507

<http://secunia.com/advisories/27507>

* SECUNIA: 27625

<http://secunia.com/advisories/27625>

* SECUNIA: 27601

<http://secunia.com/advisories/27601>

* SECUNIA: 27628

<http://secunia.com/advisories/27628>

* SECUNIA: 27780

<http://secunia.com/advisories/27780>

* SECUNIA: 27399

<http://secunia.com/advisories/27399>

* SECUNIA: 27878

<http://secunia.com/advisories/27878>

* SECUNIA: 28548

<http://secunia.com/advisories/28548>

* XF: flac-media-files-bo(37187)

<http://xforce.iss.net/xforce/xfdb/37187>

CVE Reference:

CVE-2007-4619 (cve.mitre.org, nvd.nist.gov)

• 18080 Winamp in_mp3.dll arbitrary code execution Vulnerability (Remote File Checking)

Multiple stack-based buffer overflows in in_mp3.dll in Winamp 5.21, 5.5, and 5.51 allow remote attackers to execute arbitrary code via a long (1) artist or (2) name tag in Ultravox streaming metadata, related to construction of stream titles.

The vulnerability is confirmed in version 5.x before 5.52.

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

References:

- * MISC:
http://secunia.com/secunia_research/2008-2/advisory/
- * CONFIRM:
<http://www.winamp.com/player/version-history>
- * BID: 27344
<http://www.securityfocus.com/bid/27344>
- * FRSIRT: ADV-2008-0183
<http://www.frsirt.com/english/advisories/2008/0183>
- * SECUNIA: 27865
<http://secunia.com/advisories/27865>
- * XF: winamp-inmp3-bo(39778)
<http://xforce.iss.net/xforce/xfdb/39778>

CVE Reference:

CVE-2008-0065 (cve.mitre.org, nvd.nist.gov)

• 18081 VMware Workstation, ActiveX control unspecified vulnerability (CVE-2007-5438) (Remote File Checking)

Unspecified vulnerability in a certain ActiveX control in Reconfig.DLL in VMware Workstation 5.5.x before 5.5.8 build 108000, and VMware Workstation 6.0.x before 6.0.5 build 109488, might allow local users to cause a denial of service to the Virtual Disk Mount Service (vmount2.exe), related to the ConnectPopulatedDiskEx function.

The issue is fixed in VMware Workstation 5.5.8 and 6.0.5.

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

References:

- * BUGTRAQ: 20071010 [ELEYTT] 10PAZDZIERNIK2007
<http://www.securityfocus.com/archive/1/archive/1/482021/100/0/threaded>
- * BUGTRAQ: 20080830 VMSA-2008-0014 Updates to VMware Workstation, VMware Player, VMware ACE, VMware Server, VMware ESX address information disclosure, privilege escalation and other security issues.
<http://www.securityfocus.com/archive/1/archive/1/495869/100/0/threaded>
- * FULLDISC: 20080830 VMSA-2008-0014 Updates to VMware Workstation, VMware Player, VMware ACE, VMware Server, VMware ESX address information disclosure, privilege escalation and other security issues.
<http://lists.grok.org.uk/pipermail/full-disclosure/2008-August/064118.html>
- * MISC:
http://www.eleytt.com/advisories/eleytt_VMWARE1.pdf
- * CONFIRM:
http://www.vmware.com/support/ace/doc/releasenotes_ace.html
- * CONFIRM:
http://www.vmware.com/support/ace2/doc/releasenotes_ace2.html
- * CONFIRM:
http://www.vmware.com/support/player/doc/releasenotes_player.html
- * CONFIRM:
http://www.vmware.com/support/player2/doc/releasenotes_player2.html
- * CONFIRM:
http://www.vmware.com/support/server/doc/releasenotes_server.html
- * CONFIRM:
http://www.vmware.com/support/ws55/doc/releasenotes_ws55.html
- * CONFIRM:
http://www.vmware.com/support/ws6/doc/releasenotes_ws6.html
- * BID: 26025
<http://www.securityfocus.com/bid/26025>
- * FRSIRT: ADV-2008-2466
<http://www.frsirt.com/english/advisories/2008/2466>
- * SECUNIA: 31707
<http://secunia.com/advisories/31707>
- * SECUNIA: 31708
<http://secunia.com/advisories/31708>
- * SECUNIA: 31709
<http://secunia.com/advisories/31709>
- * SECUNIA: 31710
<http://secunia.com/advisories/31710>

* SREASON: 3219

<http://securityreason.com/securityalert/3219>

CVE Reference:

CVE-2007-5438 (cve.mitre.org, nvd.nist.gov)

• 18083 VMware Workstation, ActiveX control unspecified vulnerability (CVE-2008-3691) (Remote File Checking)

Unspecified vulnerability in a certain ActiveX control in VMware Workstation 5.5.x before 5.5.8 build 108000, and VMware Workstation 6.0.x before 6.0.5 build 109488, has unknown impact and remote attack vectors.

The issue is fixed in VMware Workstation 5.5.8 and 6.0.5.

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

References:

* BUGTRAQ: 20080830 VMSA-2008-0014 Updates to VMware Workstation, VMware Player, VMware ACE, VMware Server, VMware ESX address information disclosure, privilege escalation and other security issues.

<http://www.securityfocus.com/archive/1/archive/1/495869/100/0/threaded>

* FULLDISC: 20080830 VMSA-2008-0014 Updates to VMware Workstation, VMware Player, VMware ACE, VMware Server, VMware ESX address information disclosure, privilege escalation and other security issues.

<http://lists.grok.org.uk/pipermail/full-disclosure/2008-August/064118.html>

* CONFIRM:

http://www.vmware.com/support/ace/doc/releasenotes_ace.html

* CONFIRM:

http://www.vmware.com/support/ace2/doc/releasenotes_ace2.html

* CONFIRM:

http://www.vmware.com/support/player/doc/releasenotes_player.html

* CONFIRM:

http://www.vmware.com/support/player2/doc/releasenotes_player2.html

* CONFIRM:

http://www.vmware.com/support/server/doc/releasenotes_server.html

* CONFIRM:

http://www.vmware.com/support/ws55/doc/releasenotes_ws55.html

* CONFIRM:

http://www.vmware.com/support/ws6/doc/releasenotes_ws6.html

* BID: 30934

<http://www.securityfocus.com/bid/30934>

* FRSIRT: ADV-2008-2466

<http://www.frsirt.com/english/advisories/2008/2466>

* SECUNIA: 31707

<http://secunia.com/advisories/31707>

* SECUNIA: 31708

<http://secunia.com/advisories/31708>

* SECUNIA: 31709

<http://secunia.com/advisories/31709>

* SECUNIA: 31710

<http://secunia.com/advisories/31710>

CVE Reference:

CVE-2008-3691 (cve.mitre.org, nvd.nist.gov)

• 18085 VMware Workstation, ActiveX control unspecified vulnerability (CVE-2008-3692) (Remote File Checking)

Unspecified vulnerability in a certain ActiveX control in VMware Workstation 5.5.x before 5.5.8 build 108000, VMware Workstation 6.0.x before 6.0.5 build 109488, has unknown impact and remote attack vectors.

The issue is fixed in VMware Workstation 5.5.8 and 6.0.5.

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

References:

* BUGTRAQ: 20080830 VMSA-2008-0014 Updates to VMware Workstation, VMware Player, VMware ACE, VMware Server, VMware ESX address information disclosure, privilege escalation and other security issues.

<http://www.securityfocus.com/archive/1/archive/1/495869/100/0/threaded>

* FULLDISC: 20080830 VMSA-2008-0014 Updates to VMware Workstation, VMware Player, VMware ACE, VMware Server, VMware ESX address information disclosure, privilege escalation and other security issues.

<http://lists.grok.org.uk/pipermail/full-disclosure/2008-August/064118.html>

* CONFIRM:

http://www.vmware.com/support/ace/doc/releasenotes_ace.html

* CONFIRM:

http://www.vmware.com/support/ace2/doc/releasenotes_ace2.html

* CONFIRM:

http://www.vmware.com/support/player/doc/releasenotes_player.html

* CONFIRM:

http://www.vmware.com/support/player2/doc/releasenotes_player2.html

* CONFIRM:

http://www.vmware.com/support/server/doc/releasenotes_server.html

* CONFIRM:

http://www.vmware.com/support/ws55/doc/releasenotes_ws55.html

* CONFIRM:

http://www.vmware.com/support/ws6/doc/releasenotes_ws6.html

* BID: 30934

<http://www.securityfocus.com/bid/30934>

* FRSIRT: ADV-2008-2466

<http://www.frsirt.com/english/advisories/2008/2466>

* SECUNIA: 31707

<http://secunia.com/advisories/31707>

* SECUNIA: 31708

<http://secunia.com/advisories/31708>

* SECUNIA: 31709

<http://secunia.com/advisories/31709>

* SECUNIA: 31710

<http://secunia.com/advisories/31710>

CVE Reference:

CVE-2008-3692 (cve.mitre.org, nvd.nist.gov)

• 18087 VMware Workstation, ActiveX control unspecified vulnerability (CVE-2008-3693) (Remote File Checking)

Unspecified vulnerability in a certain ActiveX control in VMware Workstation 5.5.x before 5.5.8 build 108000, VMware Workstation 6.0.x before 6.0.5 build 109488, has unknown impact and remote attack vectors.

The issue is fixed in VMware Workstation 5.5.8 and VMware Workstation 6.0.5.

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

References:

* BUGTRAQ: 20080830 VMSA-2008-0014 Updates to VMware Workstation, VMware Player, VMware ACE, VMware Server, VMware ESX address information disclosure, privilege escalation and other security issues.

<http://www.securityfocus.com/archive/1/archive/1/495869/100/0/threaded>

* FULLDISC: 20080830 VMSA-2008-0014 Updates to VMware Workstation, VMware Player, VMware ACE, VMware Server, VMware ESX address information disclosure, privilege escalation and other security issues.

<http://lists.grok.org.uk/pipermail/full-disclosure/2008-August/064118.html>

* CONFIRM:

http://www.vmware.com/support/ace/doc/releasenotes_ace.html

* CONFIRM:

http://www.vmware.com/support/ace2/doc/releasenotes_ace2.html

* CONFIRM:

http://www.vmware.com/support/player/doc/releasenotes_player.html

* CONFIRM:

http://www.vmware.com/support/player2/doc/releasenotes_player2.html

* CONFIRM:

http://www.vmware.com/support/server/doc/releasenotes_server.html

* CONFIRM:

http://www.vmware.com/support/ws55/doc/releasenotes_ws55.html

* CONFIRM:

http://www.vmware.com/support/ws6/doc/releasenotes_ws6.html

* BID: 30934

<http://www.securityfocus.com/bid/30934>

* FRSIRT: ADV-2008-2466

<http://www.frsirt.com/english/advisories/2008/2466>

* SECUNIA: 31707

<http://secunia.com/advisories/31707>

* SECUNIA: 31708

<http://secunia.com/advisories/31708>

* SECUNIA: 31709

<http://secunia.com/advisories/31709>

* SECUNIA: 31710

<http://secunia.com/advisories/31710>

CVE Reference:

CVE-2008-3693 (cve.mitre.org, nvd.nist.gov)

• 18089 VMware Workstation, ActiveX control unspecified vulnerability (CVE-2008-3694) (Remote File Checking)

Unspecified vulnerability in a certain ActiveX control in VMware Workstation 5.5.x before 5.5.8 build 108000, VMware Workstation 6.0.x before 6.0.5 build 109488, has unknown impact and remote attack vectors.

The issue is fixed in VMware Workstation 5.5.8 and VMware Workstation 6.0.5.

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

References:

* BUGTRAQ: 20080830 VMSA-2008-0014 Updates to VMware Workstation, VMware Player, VMware ACE, VMware Server, VMware ESX address information disclosure, privilege escalation and other security issues.

<http://www.securityfocus.com/archive/1/archive/1/495869/100/0/threaded>

* FULLDISC: 20080830 VMSA-2008-0014 Updates to VMware Workstation, VMware Player, VMware ACE, VMware Server, VMware ESX address information disclosure, privilege escalation and other security issues.

<http://lists.grok.org.uk/pipermail/full-disclosure/2008-August/064118.html>

* CONFIRM:

http://www.vmware.com/support/ace/doc/releasenotes_ace.html

* CONFIRM:

http://www.vmware.com/support/ace2/doc/releasenotes_ace2.html

* CONFIRM:

http://www.vmware.com/support/player/doc/releasenotes_player.html

* CONFIRM:

http://www.vmware.com/support/player2/doc/releasenotes_player2.html

* CONFIRM:

http://www.vmware.com/support/server/doc/releasenotes_server.html

* CONFIRM:

http://www.vmware.com/support/ws55/doc/releasenotes_ws55.html

* CONFIRM:

http://www.vmware.com/support/ws6/doc/releasenotes_ws6.html

* BID: 30934

<http://www.securityfocus.com/bid/30934>

* FRSIRT: ADV-2008-2466

<http://www.frsirt.com/english/advisories/2008/2466>

* SECUNIA: 31707

<http://secunia.com/advisories/31707>

* SECUNIA: 31708

<http://secunia.com/advisories/31708>

* SECUNIA: 31709

<http://secunia.com/advisories/31709>

* SECUNIA: 31710

<http://secunia.com/advisories/31710>

CVE Reference:

CVE-2008-3694 (cve.mitre.org, nvd.nist.gov)

• 18091 VMware Workstation, ActiveX control unspecified vulnerability (CVE-2008-3695) (Remote File Checking)

Unspecified vulnerability in a certain ActiveX control in VMware Workstation 5.5.x before 5.5.8 build 108000, VMware Workstation 6.0.x before 6.0.5 build 109488, has unknown impact and remote attack vectors.

The issue is fixed in VMware Workstation 5.5.8 and VMware Workstation 6.0.5.

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

References:

* BUGTRAQ: 20080830 VMSA-2008-0014 Updates to VMware Workstation, VMware Player, VMware ACE, VMware Server, VMware ESX address information disclosure, privilege escalation and other security issues.

<http://www.securityfocus.com/archive/1/archive/1/495869/100/0/threaded>

* FULLDISC: 20080830 VMSA-2008-0014 Updates to VMware Workstation, VMware Player, VMware ACE, VMware Server, VMware ESX address information disclosure, privilege escalation and other security issues.

<http://lists.grok.org.uk/pipermail/full-disclosure/2008-August/064118.html>

* CONFIRM:

http://www.vmware.com/support/ace/doc/releasenotes_ace.html

* CONFIRM:

http://www.vmware.com/support/ace2/doc/releasenotes_ace2.html

* CONFIRM:

http://www.vmware.com/support/player/doc/releasenotes_player.html

* CONFIRM:

http://www.vmware.com/support/player2/doc/releasenotes_player2.html

* CONFIRM:

http://www.vmware.com/support/server/doc/releasenotes_server.html

* CONFIRM:

http://www.vmware.com/support/ws55/doc/releasenotes_ws55.html

* CONFIRM:

http://www.vmware.com/support/ws6/doc/releasenotes_ws6.html

* BID: 30934

<http://www.securityfocus.com/bid/30934>

* FRSIRT: ADV-2008-2466

<http://www.frsirt.com/english/advisories/2008/2466>

* SECUNIA: 31707

<http://secunia.com/advisories/31707>

* SECUNIA: 31708

<http://secunia.com/advisories/31708>

* SECUNIA: 31709

<http://secunia.com/advisories/31709>

* SECUNIA: 31710

<http://secunia.com/advisories/31710>

CVE Reference:

CVE-2008-3695 (cve.mitre.org, nvd.nist.gov)

• 18093 VMware Workstation, ActiveX control unspecified vulnerability (CVE-2008-3696) (Remote File Checking)

Unspecified vulnerability in a certain ActiveX control in VMware Workstation 5.5.x before 5.5.8 build 108000, VMware Workstation 6.0.x before 6.0.5 build 109488, has unknown impact and remote attack vectors.

The issue is fixed in VMware Workstation 5.5.8 and VMware Workstation 6.0.5.

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

References:

* BUGTRAQ: 20080830 VMSA-2008-0014 Updates to VMware Workstation, VMware Player, VMware ACE, VMware Server, VMware ESX address information disclosure, privilege escalation and other security issues.

<http://www.securityfocus.com/archive/1/archive/1/495869/100/0/threaded>

* FULLDISC: 20080830 VMSA-2008-0014 Updates to VMware Workstation, VMware Player, VMware ACE, VMware Server, VMware ESX address information disclosure, privilege escalation and other security issues.

<http://lists.grok.org.uk/pipermail/full-disclosure/2008-August/064118.html>

* CONFIRM:

http://www.vmware.com/support/ace/doc/releasenotes_ace.html

* CONFIRM:

http://www.vmware.com/support/ace2/doc/releasenotes_ace2.html

* CONFIRM:

http://www.vmware.com/support/player/doc/releasenotes_player.html

* CONFIRM:

http://www.vmware.com/support/player2/doc/releasenotes_player2.html

* CONFIRM:

http://www.vmware.com/support/server/doc/releasenotes_server.html

* CONFIRM:

http://www.vmware.com/support/ws55/doc/releasenotes_ws55.html

* CONFIRM:

http://www.vmware.com/support/ws6/doc/releasenotes_ws6.html

* BID: 30934

<http://www.securityfocus.com/bid/30934>

* FRSIRT: ADV-2008-2466

<http://www.frsirt.com/english/advisories/2008/2466>

* SECUNIA: 31707
<http://secunia.com/advisories/31707>
* SECUNIA: 31708
<http://secunia.com/advisories/31708>
* SECUNIA: 31709
<http://secunia.com/advisories/31709>
* SECUNIA: 31710
<http://secunia.com/advisories/31710>

CVE Reference:

CVE-2008-3696 (cve.mitre.org, nvd.nist.gov)

• 18095 VMware Workstation, OpenProcess function unspecified vulnerability (Remote File Checking)

Unspecified vulnerability in the OpenProcess function in VMware Workstation 5.5.x before 5.5.8 build 108000, VMware Workstation 6.0.x before 6.0.5 build 109488, on Windows allows local host OS users to gain privileges on the host OS via unknown vectors.

The issue is fixed in VMware Workstation 5.5.8 and VMware Workstation 6.0.5.

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

References:

* BUGTRAQ: 20080830 VMSA-2008-0014 Updates to VMware Workstation, VMware Player, VMware ACE, VMware Server, VMware ESX address information disclosure, privilege escalation and other security issues.
<http://www.securityfocus.com/archive/1/archive/1/495869/100/0/threaded>
* FULLDISC: 20080830 VMSA-2008-0014 Updates to VMware Workstation, VMware Player, VMware ACE, VMware Server, VMware ESX address information disclosure, privilege escalation and other security issues.
<http://lists.grok.org.uk/pipermail/full-disclosure/2008-August/064118.html>
* CONFIRM:
http://www.vmware.com/support/ace/doc/releasenotes_ace.html
* CONFIRM:
http://www.vmware.com/support/ace2/doc/releasenotes_ace2.html
* CONFIRM:
http://www.vmware.com/support/player/doc/releasenotes_player.html
* CONFIRM:
http://www.vmware.com/support/player2/doc/releasenotes_player2.html
* CONFIRM:
http://www.vmware.com/support/server/doc/releasenotes_server.html
* CONFIRM:
http://www.vmware.com/support/ws55/doc/releasenotes_ws55.html
* CONFIRM:
http://www.vmware.com/support/ws6/doc/releasenotes_ws6.html
* BID: 30936
<http://www.securityfocus.com/bid/30936>
* FRSIRT: ADV-2008-2466
<http://www.frsirt.com/english/advisories/2008/2466>
* APPLE: 31707
<http://secunia.com/advisories/31707>

CVE Reference:

CVE-2008-3698 (cve.mitre.org, nvd.nist.gov)

New Vulnerabilities found this Week

• CVE-2008-3893 Microsoft CVSS 2.0 Score = 1.9

Microsoft BitLocker in Windows Vista before SP1 stores pre-boot authentication passwords in the BIOS Keyboard buffer and does not clear this buffer during boot, which allows local users to obtain sensitive information by reading the physical memory locations associated with this buffer.

Test Case Impact: Vulnerability Impact: Risk: **Low**

References:

<http://www.ivizsecurity.com/security-advisory-iviz-sr-0801.html>

SECUNIA: <http://secunia.com/advisories/31619>

CVE Reference: [CVE-2008-3893](#)

• **CVE-2008-3536 HP CVSS 2.0 Score = 7.8**

Unspecified vulnerability in ovalarmsrv in HP OpenView Network Node Manager (OV NNM) 7.01, 7.51, and 7.53 allows remote attackers to cause a denial of service via unknown vectors, a different vulnerability than CVE-2008-3537.

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

References:

HP: <http://marc.info/?l=bugtraq&m=122037165310549&w=2>

CVE Reference: [CVE-2008-3536](#)

• **CVE-2008-3537 HP CVSS 2.0 Score = 7.8**

Unspecified vulnerability in ovalarmsrv in HP OpenView Network Node Manager (OV NNM) 7.01, 7.51, and 7.53 allows remote attackers to cause a denial of service via unknown vectors, a different vulnerability than CVE-2008-3536.

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

References:

HP: <http://marc.info/?l=bugtraq&m=122037165310549&w=2>

CVE Reference: [CVE-2008-3537](#)

• **CVE-2008-3947 HP CVSS 2.0 Score = 7.2**

DCL (aka the CLI) in OpenVMS Alpha 8.3 allows local users to gain privileges via a long command line.

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

References:

MISC: <http://deathrow.vistech.net/DEFCON16/VMS.PDF>

CVE Reference: [CVE-2008-3947](#)

• **CVE-2008-3946 HP CVSS 2.0 Score = 4.9**

The finger client in HP TCP/IP Services for OpenVMS 5.x allows local users to read arbitrary files via a link corresponding to a (1) .plan or (2) .project file.

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

References:

MISC: <http://deathrow.vistech.net/DEFCON16/VMS.PDF>

CVE Reference: [CVE-2008-3946](#)

• **CVE-2008-3940 HP CVSS 2.0 Score = 4.4**

Format string vulnerability in the finger client in HP TCP/IP Services for OpenVMS 5.x allows local users to gain privileges via format string specifiers in a (1) .plan or (2) .project file.

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

References:

BID: <http://www.securityfocus.com/bid/30948>

FRSIRT: <http://www.frsirt.com/english/advisories/2008/2463>

SECUNIA: <http://secunia.com/advisories/31587>

MISC: <http://deathrow.vistech.net/DEFCON16/VMS.PDF>

CVE Reference: [CVE-2008-3940](#)

• **CVE-2008-2732 Cisco CVSS 2.0 Score = 7.8**

Multiple unspecified vulnerabilities in the SIP inspection functionality in Cisco PIX and Adaptive Security Appliance (ASA) 5500 devices 7.0 before 7.0(7)16, 7.1 before 7.1(2)71, 7.2 before 7.2(4)7, 8.0 before 8.0(3)20, and 8.1 before 8.1(1)8 allow remote attackers to cause a denial of service (device reload) via unknown vectors, aka Bug IDs CSCsq07867, CSCsq57091, CSCsk60581, and CSCsq39315.

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

References:

SECTRAK: <http://www.securitytracker.com/id?1020809>

SECTRAK: <http://www.securitytracker.com/id?1020808>

CISCO: http://www.cisco.com/en/US/products/products_security_advisory09186a00809f138a.shtml

CVE Reference: [CVE-2008-2732](#)

• **CVE-2008-2441 Cisco CVSS 2.0 Score = 7.5**

Cisco Secure ACS 3.x before 3.3(4) Build 12 patch 7, 4.0.x, 4.1.x before 4.1(4) Build 13 Patch 11, and 4.2.x before 4.2(0) Build 124 Patch 4 does not properly handle an EAP Response packet in which the value of the length field exceeds the actual packet length, which allows remote authenticated users to cause a denial of service (CSRadius and CSAuth service crash) or possibly execute arbitrary code via a crafted RADIUS (1) EAP-Response/Identity, (2) EAP-Response/MD5, or (3) EAP-Response/TLS Message Attribute packet.

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

References:

SECTRAK: <http://www.securitytracker.com/id?1020814>

BUGTRAQ: <http://www.securityfocus.com/archive/1/archive/1/495937/100/0/threaded>

CISCO: <http://www.cisco.com/warp/public/707/cisco-sr-20080903-csacs.shtml>

CVE Reference: [CVE-2008-2441](#)

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