netVigilance
assurance has arrived

ScoutNews

The weekly Security update from the makers of SecureScout

2006 Issue # 38

September 22, 2006

Table of Contents

Product Focus

CodeRed Worm Scanner – The CodeRed Worm Scanner is a free utility made by SecureScout that will scan up to 256 IP addresses at once to assess if any have been infected by CodeRed Worm.

This Week in Review

Tightened security in VISTA. Portable devices pose serious security risks. IPv6 and security. Review of 'Computer Security Basics'.

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

- **Microsoft gets credit for tightening security**

High-profile worms were 'real wake-up calls' at Microsoft, says security program manager

CodeRed, Nimda, and Blaster. These high-profile worms, which exploited flaws in Microsoft's Windows operating system and other applications, made Microsoft the butt of security jokes and forced the company to reexamine its approach to developing secure software.
Throughout Microsoft, we thought Windows 2000 was a very solid, reliable operating

system, perfect for deployment in the enterprise," said Ian Hellen, a security program manager at Microsoft's Windows Security Engineering Team. "Those tiny pieces of code were real wake-up calls, saying Windows 2000 isn't there yet. It's just not designed to cope with these kinds of threats."

That was then. With the commercial release of Vista just months away, Microsoft's efforts to improve security are now showing results, though much remains to be done by the company, said security experts attending the Hack In The Box Security Conference (HITB) in Kuala Lumpur, Malaysia, this week.

InfoWorld

Full Story :
http://www.infoworld.com/article/06/09/22/HNmstightensecurity_1.html?source=rss&url=http://www.infoworld.com/article/06/09/22/HNmstightensecurity_1.html

❖ Pod slurping can lead to major security breaches

Information theft has now become a major concern for every organization and thus data leakage prevention is slowly taking up a bigger portion of the IT budget. This drive is attributed to two factors: The wave of malevolent threats that is hitting every industry and the increase in regulatory requirements which demand more protection and tighter controls over client records and other confidential information. More stringent controls and severe penalties are forcing organizations to address regulatory compliance more seriously

A misconception shared by many organizations is that security threats mostly originate from outside the corporation. In fact, countless dollars are being spent every year on firewalls and other solutions that secure the corporate perimeter from external threats. However statistics show that internal security breaches are growing faster than external attacks and at least half of security breaches originate from behind the corporate firewall.

SecurityPark.net

Full Story :
http://www.securitypark.co.uk/article.asp?articleid=25862&CategoryID=1

❖ Get to grips with IPv6 security issues, warns expert

Sysadmins need to start looking at the security implicatiosn of IPv6, a security consultant has warned.
For many IT managers, the next version of the Internet Protocol seems like a far-off concern. But the technology will make its way into corporate IT systems sooner than many people realise, forcing IT departments to confront potential security vulnerabilities, Van Hauser, a security consultant and the founder of hacking group The Hacker's Choice, has warned.

Companies need to prepare themselves for IPv6, even if they don't have plans to upgrade their networks, said Hauser as he discussed security vulnerabilities during a presentation at the Hack In The Box Security Conference (HITB) in Kuala Lumpur, Malaysia.

"Most people think there's no IPv6 now, so where's the problem?" Hauser said. "The thing is if you install any Unix operating system now it comes with IPv6 enabled." Microsoft's Vista operating system will also have support for IPv6 enabled.

TechWorld

Full Story :
http://www.techworld.com/security/news/index.cfm?newsID=6942&pagtype=samechan

- **REVIEW: "Computer Security Basics", Lehtinen/Russell/Gangemi**

I've been waiting a long time for an updated version of this classic.

"Computer Security Basics" was a pretty accurate name for the first edition. The book was an overview of many aspects that go into the security of computers and data systems. While not exhaustive, it provided a starting point from which to pursue specific topics that required more detailed study. Such is no longer the case.

Part one looks at security for today. Chapter one starts with 9/11, then talks about various infosec groups, and only then gets to an introduction of what security is, and how to evaluate potential loopholes. The definition points out the useful difference between the problems of confidentiality and availability, and now adds integrity. The distinction between threats, vulnerabilities and countermeasures is helpful, but may fail to resolve certain issues. Ironically, in view of the title of this section, chapter two gives some historical background to the development of modern data security.

Part two deals with computer security itself. Chapter three looks at access control, but is somewhat unstructured. Malware and viruses receive the all-too-usual mix of advice and inaccuracies in chapter four. Policy is supposed to be the topic of chapter five, but most of the text is concerned with matters of operations. Internet and Web technologies, and a few network attacks, are listed in chapter six.

RISKS Digest

Full Story :
http://catless.ncl.ac.uk/go/risks/24/43/16

New Vulnerabilities Tested in SecureScout

- **14737 Mozilla Firefox error in the handling of JavaScript regular expressions, arbitrary code execution (Remote File Checking)**

A vulnerability has been reported in Mozilla Firefox, which can be exploited by malicious people to compromise a user's system.

An error in the handling of JavaScript regular expressions containing a minimal quantifier can be exploited to cause a heap-based buffer overflow.

Successful exploitation may allow execution of arbitrary code.

The weakness has been confirmed in version 1.5.0.6. Other versions may also be affected.

Test Case Impact: **Gather Info.** Vulnerability Impact: **Attack** Risk: **Medium**

References:

Original Advisory:
http://www.mozilla.org/security/announce/2006/mfsa2006-57.html

Other references:
REDHAT:RHSA-2006:0676
URL:http://www.redhat.com/support/errata/RHSA-2006-0676.html
REDHAT:RHSA-2006:0677
URL:http://www.redhat.com/support/errata/RHSA-2006-0677.html
REDHAT:RHSA-2006:0675
URL:http://www.redhat.com/support/errata/RHSA-2006-0675.html
BID:20042
URL:http://www.securityfocus.com/bid/20042
FRSIRT:ADV-2006-3617
URL:http://www.frsirt.com/english/advisories/2006/3617
SECTRACK:1016846
URL:http://securitytracker.com/id?1016846
SECTRACK:1016847
URL:http://securitytracker.com/id?1016847
SECTRACK:1016848
URL:http://securitytracker.com/id?1016848
SECUNIA:21906
URL:http://secunia.com/advisories/21906
SECUNIA:21949
URL:http://secunia.com/advisories/21949
SECUNIA:21915
URL:http://secunia.com/advisories/21915
SECUNIA:21916
URL:http://secunia.com/advisories/21916
SECUNIA:21939
URL:http://secunia.com/advisories/21939
SECUNIA:21940
URL:http://secunia.com/advisories/21940
SECUNIA:21950
URL:http://secunia.com/advisories/21950
XF:mozilla-javascript-expression-bo(28955)
URL:http://xforce.iss.net/xforce/xfdb/28955

Product HomePage:
http://www.mozilla.org/products/firefox/

CVE Reference: CVE-2006-4565

❖ **14738 Mozilla Firefox auto-update mechanism self-signed certificates easy acceptation (Remote File Checking)**

A vulnerability has been reported in Mozilla Firefox, which can be exploited by malicious people to conduct man-in-the-middle attacks.

The auto-update mechanism uses SSL to communicate securely. The problem is that users may have accepted an unverifiable self-signed certificate when visiting a web site, which will allow an attacker to redirect the update check to a malicious web site in a man-in-the-middle attack.

The weakness has been confirmed in version 1.5.0.6. Other versions may also be affected.

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

References:

Original Advisory:
http://www.mozilla.org/security/announce/2006/mfsa2006-58.html

Other references:
REDHAT:RHSA-2006:0677
URL:http://www.redhat.com/support/errata/RHSA-2006-0677.html
REDHAT:RHSA-2006:0675
URL:http://www.redhat.com/support/errata/RHSA-2006-0675.html
BID:20042
URL:http://www.securityfocus.com/bid/20042
FRSIRT:ADV-2006-3617
URL:http://www.frsirt.com/english/advisories/2006/3617
SECTRACK:1016850
URL:http://securitytracker.com/id?1016850
SECTRACK:1016851
URL:http://securitytracker.com/id?1016851
SECUNIA:21906
URL:http://secunia.com/advisories/21906
SECUNIA:21949
URL:http://secunia.com/advisories/21949
SECUNIA:21916
URL:http://secunia.com/advisories/21916
SECUNIA:21939
URL:http://secunia.com/advisories/21939
SECUNIA:21950
URL:http://secunia.com/advisories/21950
XF:mozilla-auto-update-gain-access(28950)
URL:http://xforce.iss.net/xforce/xfdb/28950

Product HomePage:
http://www.mozilla.org/products/firefox/

CVE Reference: CVE-2006-4567

❖ 14739 Mozilla Firefox time-dependent errors, memory corruption (Remote File Checking)

A vulnerability has been reported in Mozilla Firefox, which can be exploited by

malicious people to execute arbitrary code.
Some time-dependent errors during text display can be exploited to corrupt memory.
Successful exploitation may allow execution of arbitrary code.
The weakness has been confirmed in version 1.5.0.6. Other versions may also be affected.

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

References:

Original Advisory:
http://www.mozilla.org/security/announce/2006/mfsa2006-59.html

Product HomePage:
http://www.mozilla.org/products/firefox/

CVE Reference: CVE-2006-4253

❖ 14740 Mozilla Firefox error within the verification of certain signatures in NSS library (Remote File Checking)

A vulnerability has been reported in Mozilla Firefox, which can be exploited by malicious people to bypass certain security restrictions.

A vulnerability has been reported in Network Security Services (NSS), which potentially can be exploited by malicious people to bypass certain security restrictions.

The weakness has been confirmed in version 1.5.0.6. Other versions may also be affected.

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

References:

Original Advisory:
http://www.mozilla.org/security/announce/2006/mfsa2006-60.html

Product HomePage:
http://www.mozilla.org/products/firefox/

CVE Reference: CVE-2006-4340

❖ 14741 Mozilla Firefox error in the cross-domain handling, HTML and script code injection (Remote File Checking)

A vulnerability has been reported in Mozilla Firefox, which can be exploited by malicious people to inject arbitrary HTML and script code.

An error in the cross-domain handling can be exploited to inject arbitrary HTML and

script code in a sub-frame of another web site via a "[window].frames[index].document.open()" call.

The weakness has been confirmed in version 1.5.0.6. Other versions may also be affected.

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

References:

Original Advisory:
http://www.mozilla.org/security/announce/2006/mfsa2006-61.html

Other references:
REDHAT:RHSA-2006:0676
URL:http://www.redhat.com/support/errata/RHSA-2006-0676.html
REDHAT:RHSA-2006:0675
URL:http://www.redhat.com/support/errata/RHSA-2006-0675.html
BID:20042
URL:http://www.securityfocus.com/bid/20042
FRSIRT:ADV-2006-3617
URL:http://www.frsirt.com/english/advisories/2006/3617
SECTRACK:1016855
URL:http://securitytracker.com/id?1016855
SECTRACK:1016856
URL:http://securitytracker.com/id?1016856
SECUNIA:21906
URL:http://secunia.com/advisories/21906
SECUNIA:21949
URL:http://secunia.com/advisories/21949
SECUNIA:21915
URL:http://secunia.com/advisories/21915
SECUNIA:21940
URL:http://secunia.com/advisories/21940
SECUNIA:21950
URL:http://secunia.com/advisories/21950
XF:mozilla-documentopen-frame-spoofing(28961)
URL:http://xforce.iss.net/xforce/xfdb/28961

Product HomePage:
http://www.mozilla.org/products/firefox/

CVE Reference: CVE-2006-4568

❖ 14742 Mozilla Firefox blocked popups opened in an incorrect context, HTML and script code Execution (Remote File Checking)

A vulnerability has been reported in Mozilla Firefox, which can be exploited by malicious people to inject arbitrary HTML and script code.

An error exists due to blocked popups opened from the status bar via the "blocked popups" functionality being opened in an incorrect context in certain situations. This may be exploited to execute arbitrary HTML and script code in a user's browser session in context of an arbitrary web site.

The weakness has been confirmed in version 1.5.0.6. Other versions may also be affected.

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

References:

Original Advisory:
http://www.mozilla.org/security/announce/2006/mfsa2006-62.html

Other references:
REDHAT:RHSA-2006:0675
URL:http://www.redhat.com/support/errata/RHSA-2006-0675.html
BID:20042
URL:http://www.securityfocus.com/bid/20042
SECTRACK:1016849
URL:http://securitytracker.com/id?1016849
SECUNIA:21949
URL:http://secunia.com/advisories/21949
SECUNIA:21950
URL:http://secunia.com/advisories/21950
XF:firefox-popup-blocker-xss(28957)
URL:http://xforce.iss.net/xforce/xfdb/28957

Product HomePage:
http://www.mozilla.org/products/firefox/

CVE Reference: CVE-2006-4569

❖ 14743 Mozilla Firefox memory corruption errors, arbitrary code execution (Remote File Checking)

A vulnerability has been reported in Mozilla Firefox, which can be exploited by malicious people to cause a denial of service (crash), corrupt memory, and possibly execute arbitrary code.

Multiple unspecified vulnerabilities in Firefox before 1.5.0.7, Thunderbird before 1.5.0.7, and SeaMonkey before 1.0.5 allow remote attackers to cause a denial of service (crash), corrupt memory, and possibly execute arbitrary code via unspecified vectors, some of which involve JavaScript, and possibly large images or plugin data.

The weakness has been confirmed in version 1.5.0.6. Other versions may also be affected.

Test Case Impact: **Gather Info.** Vulnerability Impact: **DoS** Risk: **High**

References:

Original Advisory:
http://www.mozilla.org/security/announce/2006/mfsa2006-64.html

Other references:
REDHAT:RHSA-2006:0676
URL:http://www.redhat.com/support/errata/RHSA-2006-0676.html
REDHAT:RHSA-2006:0677
URL:http://www.redhat.com/support/errata/RHSA-2006-0677.html
REDHAT:RHSA-2006:0675
URL:http://www.redhat.com/support/errata/RHSA-2006-0675.html
BID:20042
URL:http://www.securityfocus.com/bid/20042
FRSIRT:ADV-2006-3617
URL:http://www.frsirt.com/english/advisories/2006/3617
SECTRACK:1016846
URL:http://securitytracker.com/id?1016846
SECTRACK:1016847
URL:http://securitytracker.com/id?1016847
SECTRACK:1016848
URL:http://securitytracker.com/id?1016848
SECUNIA:21906
URL:http://secunia.com/advisories/21906
SECUNIA:21949
URL:http://secunia.com/advisories/21949
SECUNIA:21915
URL:http://secunia.com/advisories/21915
SECUNIA:21916
URL:http://secunia.com/advisories/21916
SECUNIA:21939
URL:http://secunia.com/advisories/21939
SECUNIA:21940
URL:http://secunia.com/advisories/21940
SECUNIA:21950
URL:http://secunia.com/advisories/21950

Product HomePage:
http://www.mozilla.org/products/firefox/

CVE Reference: CVE-2006-4571

❖ 16337 Vulnerability in Vector Markup Language Could Allow Remote Code Execution (925568) (Remote File Checking)

A vulnerability has been discovered in Microsoft Windows, which can be exploited by malicious people to compromise a user's system.

The vulnerability is caused due to a boundary error in the Microsoft Vector Graphics Rendering(VML) library (vgx.dll) when processing certain content in Vector Markup Language (VML) documents. This can be exploited to cause a stack-based buffer overflow by e.g. tricking a user into viewing a malicious VML document containing an overly long "fill" method inside a "rect" tag with the Internet Explorer browser.

Successful exploitation allows execution of arbitrary code with the privileges of the

application using the vulnerable functionality in the library.

NOTE: The vulnerability is currently being actively exploited.

The vulnerability is confirmed on a fully patched Microsoft Windows XP SP2 system. Other versions may also be affected.

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

References:

Original advisory:
http://www.microsoft.com/technet/security/advisory/925568.mspx

Other references:
MISC: http://sunbeltblog.blogspot.com/2006/09/seen-in-wild-zero-day-exploit-being.html
CERT-VN:VU#416092
URL:http://www.kb.cert.org/vuls/id/416092
BID:20096
URL:http://www.securityfocus.com/bid/20096
FRSIRT:ADV-2006-3679
URL:http://www.frsirt.com/english/advisories/2006/3679
SECTRACK:1016879
URL:http://securitytracker.com/id?1016879
SECUNIA:21989
URL:http://secunia.com/advisories/21989
XF:ie-vml-bo(29004)
URL:http://xforce.iss.net/xforce/xfdb/29004

CVE Reference: CVE-2006-4868

❖ 16338 Vulnerability in the Microsoft DirectAnimation Path ActiveX Control Could Allow Remote Code Execution (925444) (Remote File Checking)

nop has discovered a vulnerability in Internet Explorer, which can be exploited by malicious people to compromise a user's system.

The vulnerability is caused due to a memory corruption error in the Microsoft Multimedia Controls ActiveX control (daxctle.ocx) in the "CPathCtl::KeyFrame()" function. This can be exploited by e.g. tricking a user into viewing a malicious HTML document passing specially crafted arguments to the ActiveX control's "KeyFrame()" method.

Successful exploitation allows execution of arbitrary code.

NOTE: A somewhat working exploit is publicly available for partially patched versions of Windows 2000.

It is also possible to crash the browser via the "Spline()" method.

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

References:

Original advisory:
http://www.microsoft.com/technet/security/advisory/925444.mspx

Other references:
* BUGTRAQ:20060913 [0day] daxctle2.c - Internet Explorer COM Object Heap Overflow Download Exec Exploit
* URL:http://www.securityfocus.com/archive/1/archive/1/445898/100/0/threaded
* BUGTRAQ:20060915 Fwd: IE ActiveX 0day?
* URL:http://www.securityfocus.com/archive/1/archive/1/446065/100/0/threaded
* BUGTRAQ:20060915 RE: IE ActiveX 0day?
* URL:http://www.securityfocus.com/archive/1/archive/1/446084/100/0/threaded
* BUGTRAQ:20060915 Re: Fwd: IE ActiveX 0day?
* URL:http://www.securityfocus.com/archive/1/archive/1/446085/100/0/threaded
* MISC: http://www.milw0rm.com/exploits/2358
* MISC: http://www.xsec.org/index.php?module=releases&act=view&type=2&id=20
* CERT-VN:VU#377369
* URL:http://www.kb.cert.org/vuls/id/377369
* BID:20047
* URL:http://www.securityfocus.com/bid/20047
* FRSIRT:ADV-2006-3593
* URL:http://www.frsirt.com/english/advisories/2006/3593
* OSVDB:28842
* URL:http://www.osvdb.org/28842
* SECTRACK:1016854
* URL:http://securitytracker.com/id?1016854
* SECUNIA:21910
* URL:http://secunia.com/advisories/21910
* XF:ie-directanimation-code-execution(28942)
* URL:http://xforce.iss.net/xforce/xfdb/28942
* BUGTRAQ:20060827 [XSec-06-10]: Internet Explorer (daxctle.ocx) Heap Overflow Vulnerability
* URL:http://www.securityfocus.com/archive/1/archive/1/444504/100/0/threaded
* MISC: http://www.xsec.org/index.php?module=releases&act=view&type=1&id=19
* BID:19738
* URL:http://www.securityfocus.com/bid/19738
* OSVDB:28841
* URL:http://www.osvdb.org/28841
* SECTRACK:1016764
* URL:http://securitytracker.com/id?1016764
* XF:ie-daxctle-dos(28608)
* URL:http://xforce.iss.net/xforce/xfdb/28608

CVE Reference: CVE-2006-4777

❖ 16339 Linux Kernel SCTP Denial of Service Vulnerability

A vulnerability has been reported in the Linux Kernel, which can be exploited by malicious, local users to cause a DoS (Denial of Service).

The vulnerability is caused due to an error within the handling of SCTP sockets. This can be exploited to crash the Kernel by opening a SCTP socket with a special SO_LINGER

value.

The vulnerability has been reported in versions 2.6.17.10 and 2.6.17.11 and 2.6.18-rc5.

Test Case Impact: **Gather Info.** Vulnerability Impact: **DoS** Risk: **Low**

References:

Original advisory:
BID:20087
http://www.securityfocus.com/bid/20087

Other references:
MISC: http://www.mail-archive.com/kernel-svn-changes@lists.alioth.debian.org/msg02314.html
MISC: https://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=204460
UBUNTU:USN-347-1
URL:http://www.ubuntu.com/usn/usn-347-1

Product Homepage:
http://kernel.org/

CVE Reference: CVE-2006-4535

New Vulnerabilities found this Week

Internet Explorer daxctle.ocx "KeyFrame()" Method Vulnerability

"Execution of arbitrary code"

nop has discovered a vulnerability in Internet Explorer, which can be exploited by malicious people to compromise a user's system.

The vulnerability is caused due to a memory corruption error in the Microsoft Multimedia Controls ActiveX control (daxctle.ocx) in the "CPathCtl::KeyFrame()" function. This can be exploited by e.g. tricking a user into viewing a malicious HTML document passing specially crafted arguments to the ActiveX control's "KeyFrame()" method.

Successful exploitation allows execution of arbitrary code.

It is also possible to crash the browser via the "Spline()" method.

References:
http://www.microsoft.com/technet/security/advisory/925444.mspx
http://descriptions.securescout.com/tc/16338

Microsoft Vector Graphics Rendering Library Buffer Overflow

"Execution of arbitrary code"

A vulnerability has been discovered in Microsoft Windows, which can be exploited by malicious people to compromise a user's system.

The vulnerability is caused due to a boundary error in the Microsoft Vector Graphics Rendering(VML) library (vgx.dll) when processing certain content in Vector Markup Language (VML) documents. This can be exploited to cause a stack-based buffer overflow by e.g. tricking a user into viewing a malicious VML document containing an overly long "fill" method inside a "rect" tag with the Internet Explorer browser.

Successful exploitation allows execution of arbitrary code with the privileges of the application using the vulnerable functionality in the library.

NOTE: The vulnerability is currently being actively exploited.

The vulnerability is confirmed on a fully patched Microsoft Windows XP SP2 system. Other versions may also be affected.

References:
http://www.microsoft.com/technet/security/advisory/925568.mspx
http://www.kb.cert.org/vuls/id/416092
http://descriptions.securescout.com/tc/16337

Mozilla Firefox Multiple Vulnerabilities
"Conduct man-in-the-middle, spoofing, and cross-site scripting attacks"

Some vulnerabilities have been reported in Mozilla Firefox, which can be exploited by malicious people to conduct man-in-the-middle, spoofing, and cross-site scripting attacks, and potentially compromise a user's system.

1) An error in the handling of JavaScript regular expressions containing a minimal quantifier can be exploited to cause a heap-based buffer overflow.

Successful exploitation may allow execution of arbitrary code.

2) The auto-update mechanism uses SSL to communicate securely. The problem is that users may have accepted an unverifiable self-signed certificate when visiting a web site, which will allow an attacker to redirect the update check to a malicious web site in a man-in-the-middle attack.

3) Some time-dependent errors during text display can be exploited to corrupt memory.

Successful exploitation may allow execution of arbitrary code.

4) An error exists within the verification of certain signatures in the bundled Network Security Services (NSS) library.

5) An error in the cross-domain handling can be exploited to inject arbitrary HTML and script code in a sub-frame of another web site via a "[window].frames[index].document.open()" call.

6) An error exists due to blocked popups opened from the status bar via the "blocked popups" functionality being opened in an incorrect context in certain situations. This may be exploited to execute arbitrary HTML and script code in a user's browser session in context of an arbitrary web site.

7) Some unspecified memory corruption errors may be exploited to execute arbitrary

code.

References:
http://www.mozilla.org/security/announce/2006/mfsa2006-57.html
http://www.mozilla.org/security/announce/2006/mfsa2006-58.html
http://www.mozilla.org/security/announce/2006/mfsa2006-59.html
http://www.mozilla.org/security/announce/2006/mfsa2006-60.html
http://www.mozilla.org/security/announce/2006/mfsa2006-61.html
http://www.mozilla.org/security/announce/2006/mfsa2006-62.html
http://www.mozilla.org/security/announce/2006/mfsa2006-64.html
http://descriptions.securescout.com/tc/14737
http://descriptions.securescout.com/tc/14738
http://descriptions.securescout.com/tc/14739
http://descriptions.securescout.com/tc/14740
http://descriptions.securescout.com/tc/14741
http://descriptions.securescout.com/tc/14742
http://descriptions.securescout.com/tc/14743

Cisco Intrusion Prevention System Fragmented IP Packets Security Bypass

"Bypass the Intrusion Prevention System"

A vulnerability has been reported in Cisco Intrusion Prevention System, which can be exploited by malicious people to bypass certain security restrictions.

The vulnerability is caused due to insufficient inspection of fragmented IP packets. This can be exploited to bypass the Intrusion Prevention System to e.g. access internal systems by sending specially crafted IP packets.

The vulnerability affects the following products:
- Cisco IPS 5.0(x) software prior to 5.0(6p2)
- Cisco IPS 5.1(x) software prior to 5.1(2)

References:
http://www.cisco.com/warp/public/707/cisco-sa-20060920-ips.shtml

gzip Multiple Vulnerabilities

"Denial of Service"

Tavis Ormandy has reported some vulnerabilities in gzip, which can be exploited by malicious people to cause a DoS (Denial of Service) and potentially compromise a vulnerable system.

1) A boundary error within the "make_table()" function in unlzh.c can be used to modify certain stack data. This can be exploited to cause a DoS and potentially allows to execute arbitrary code by e.g. tricking a user or automated system into unpacking a specially crafted archive file.

2) A buffer underflow exists within the "build_tree()" function in unpack.c, which can be exploited to cause a DoS and potentially allows to execute arbitrary code by e.g. tricking a user or automated system into unpacking a specially crafted "pack" archive file.

3) A buffer overflow within the "make_table()" function of gzip's LZH support can be

exploited to cause a DoS and potentially to compromise a vulnerable system by e.g. tricking a user or automated system into unpacking an archive containing a specially crafted decoding table.

4) A NULL pointer dereference within the "huft_build()" function and an infinite loop within the LZH handling can be exploited to cause a DoS by e.g. tricking a user or automated system into unpacking a specially crafted archive file.

The vulnerabilities have been reported in version 1.3.5. Other versions may also be affected.

References:
http://bugzilla.redhat.com/bugzilla/show_bug.cgi?id=204676

MailEnable SPF Lookup Denial of Service
"Denial of Service"

A vulnerability has been reported in MailEnable, which can be exploited by malicious people to cause a DoS (Denial of Service).

The vulnerability is caused due to a NULL pointer dereference error in the SMTP service when under certain circumstances processing SPF lookups. This can be exploited by performing an SPF lookup for a domain with large records.

Successful exploitation crashes the SMTP service.

References:
http://www.mailenable.com/hotfix/MESMTPC.ZIP

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