

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

[WinArpd v1.0b8](#) - Download WinArpd executable by filling our download form. Size: 55KB

Download Here:

<http://www.netvigilance.com/productdownloads?productname=winarpd.exe.zip>

This Week in Review

The most sophisticated trojan so far. Malware is a booming business. And so is protecting against it. Cloud computing and resources.

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

• Banking Trojan steals money from under your nose

Researchers at security firm Finjan have discovered details of a new type of banking Trojan horse that doesn't just steal your bank log in credentials but actually steals money from your account while you are logged in and displays a fake balance.

The bank Trojan, dubbed URLZone, has features designed to thwart fraud detection systems which are triggered by unusual transactions, Yuval Ben-Itzhak, chief technology officer at Finjan, said in an interview on Tuesday. For instance, the software is programmed to calculate on-the-fly how much money to steal from an account based on how much money is available.

It exploits a hole in Firefox, Internet Explorer 6, IE7, IE8 and Opera, said Ben-Itzhak. Cnet Security

Full Story :

http://news.cnet.com/8301-27080_3-10363836-245.html?part=rss&subj=news&tag=2547-1_3-0-20

• Adware pushers evolve into malware distribution channel

An industry built on serving adware has become a full-fledged malware distribution channel, with a thriving underground economy, according to researchers at SecureWorks.

The business model is known as pay-per-install (PPI), and profits by recruiting "affiliates" willing to facilitate malware installation on victims' computers.

According to a new report from the SecureWorks Counter Threat Unit titled "The Underground Economy of the Pay-Per-Install Business," the method begins when an affiliate interested in building a network of infected computers signs up to a PPI site and receives files from the PPI provider. SC Magazine

Full Story :

<http://www.scmagazineus.com/Adware-pushers-evolve-into-malware-distribution-channel/article/151090/>

• DHS to hire up to 1,000 cybersecurity experts

The U.S. Department of Homeland Security plans to hire up to 1,000 people to fill cybersecurity jobs across the agency, Secretary Janet Napolitano announced Thursday.

The new positions, to be filled during the next three years, will involve roles in cyber-risk and analysis; incident response; vulnerability discovery and assessment; intelligence and investigation and systems engineering, said Napolitano, whose announcement coincided with the start of National Cybersecurity Awareness Month.

"Effective cybersecurity requires all partners -- individuals, communities, government entities and the private sector -- to work together to protect our networks and strengthen our cyber-resiliency," Napolitano said in a statement. "This new hiring authority will enable DHS to recruit the best cyberanalysts, developers and engineers in the world to serve their country by leading the nation's defenses against cyberthreats." SC Magazine

Full Story :

<http://www.scmagazineus.com/DHS-to-hire-up-to-1000-cybersecurity-experts/article/151208/>

• Cloud computing and the big rethink: Part 2

In the opening post of this series, I joined Chris Hoff and others in arguing that cloud computing will change the way we package server software, with an emphasis in lean "just enough" systems software. This means that the big, all-purpose operating system of the past will either change dramatically or disappear altogether, as the need for a "handle all comers" systems infrastructure is redistributed both up and down the execution stack.

The reduced need for specialized software packaged with bloated operating systems in turn means the virtual server is a temporary measure; a stopgap until software "containers" adjust to the needs of the cloud-computing model. In this post, I want to highlight a second reason why server virtualization (and storage and network virtualization) will give way to a new form of resource virtualization. Cnet Security

Full Story :

http://news.cnet.com/8301-19413_3-10365278-240.html?part=rss&subj=news&tag=2547-1_3-0-20

New Vulnerabilities Tested in SecureScout

• 18533 Cisco IOS Software Network Time Protocol Packet Vulnerability (cisco-sa-20090923-ntp)

When a Cisco IOS Software device supporting NTPv4 receives a specific NTP packet it will crash while creating the NTP reply packet. The NTP packet can be sent from any remote device, and does not require authentication. Cisco IOS devices supporting NTPv4 and configured with NTP peer authentication are still vulnerable. The device does not have to be explicitly configured for NTPv4 peers.

This vulnerability is documented in the following Cisco Bug IDs: CSCsu24505, and CSCsv75948. Both Cisco bug IDs are required for a full fix to this vulnerability.

Test Case Impact: **Gather Info** Vulnerability Impact: **DoS / Crash** Risk: **High**

References:

* CONFIRM:

<http://tools.cisco.com/security/center/viewAlert.x?alertId=18889>

* CISCO: 20090923 Cisco IOS Software Network Time Protocol Packet Vulnerability

http://www.cisco.com/en/US/products/products_security_advisory09186a0080af8131.shtml

* OSVDB: 58342

<http://osvdb.org/58342>

* SECTRAK: 1022930

<http://www.securitytracker.com/id?1022930>

* VUPEN: ADV-2009-2759

CVE Reference:

CVE-2009-2869 (cve.mitre.org, nvd.nist.gov)

• 18534 Cisco IOS Software Zone-Based Policy Firewall Vulnerability (cisco-sa-20090923-ios-fw)

Firewalls are networking devices that control access to the network assets of an organization. Firewalls are often positioned at the entrance points into networks. Cisco IOS software provides a set of security features that enable you to configure a simple or elaborate firewall policy, according to your particular requirements.

SIP inspection in the Cisco IOS Firewall provides basic SIP inspect functionality (SIP packet inspection and pinhole opening) as well as protocol conformance and application security.

Cisco IOS Software that is configured with Cisco IOS Zone-Based Policy Firewall SIP inspection are vulnerable to a DoS attack when processing a specific SIP transit packet. Exploitation of this vulnerability will result in a reload of the affected device.

Cisco IOS Zone-Based Policy Firewall SIP inspection was first introduced in Cisco IOS Software versions 12.4(15)XZ and 12.4(20)T.

Cisco IOS Firewall CBAC support for SIP inspection by way of the ip inspect name [inspection_name] sip is not vulnerable.

This vulnerability is documented in the following Cisco Bug ID: CSCsr18691.

Test Case Impact: **Gather Info** Vulnerability Impact: **DoS / Crash** Risk: **High**

References:

* CONFIRM:

<http://tools.cisco.com/security/center/viewAlert.x?alertId=18886>

* CISCO: 20090923 Cisco IOS Software Zone-Based Policy Firewall Vulnerability

http://www.cisco.com/en/US/products/products_security_advisory09186a0080af8130.shtml

* SECTRAK: 1022930

<http://www.securitytracker.com/id?1022930>

* VUPEN: ADV-2009-2759

<http://www.vupen.com/english/advisories/2009/2759>

CVE Reference:

CVE-2009-2867 (cve.mitre.org, nvd.nist.gov)

• 18535 Cisco IOS Software Authentication Proxy Vulnerability (cisco-sa-20090923-auth-proxy)

The Cisco IOS Firewall authentication proxy feature allows network administrators to apply specific security policies on a per-user basis. With the authentication proxy feature, users can log in to the network or access the Internet via HTTP, and their specific access profiles are automatically retrieved and applied from a CiscoSecure ACS, or other RADIUS or TACACS+ authentication server. The user profiles are active only when there is active traffic from the authenticated users. Web Authentication feature leverages the underlying authentication proxy feature.

The consent feature for Cisco IOS routers enables organizations to provide temporary Internet and corporate access to end users through their wired and wireless networks by presenting a consent webpage. The consent feature can be used with or without requesting a username and password, but still leverages the underlying authentication proxy feature.

This vulnerability allows a session to be permitted without first being authenticated by the authentication proxy, or to be permitted without first acknowledging the consent webpage. At least one successfully authenticated session or accepted consent session must exist for the vulnerability to be exposed. When this occurs, the RADIUS or TACACS+ server will show subsequent users as authenticated, all with the same username as the initial connection if performing authentication, regardless of the authentication information provided by the user and whether it was defined on the AAA server, and regardless of whether the password was correct.

This vulnerability is caused by a race condition in the code, and several conditions outside the control of a malicious user and must be met before this vulnerability could be exploited.

This vulnerability is documented in the following Cisco Bug ID: CSCsy15227.

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

References:

* CONFIRM:
<http://tools.cisco.com/security/center/viewAlert.x?alertId=18882>
* CISCO: 20090923 Cisco IOS Software Authentication Proxy Vulnerability
http://www.cisco.com/en/US/products/products_security_advisory09186a0080af8132.shtml
* BID: 36491
<http://www.securityfocus.com/bid/36491>
* OSVDB: 58340
<http://osvdb.org/58340>
* SECTRAK: 1022935
<http://www.securitytracker.com/id?1022935>
* XF: ciscoios-authenticationproxy-sec-bypass(53453)
<http://xforce.iss.net/xforce/xfdb/53453>

CVE Reference:

CVE-2009-2863 (cve.mitre.org, nvd.nist.gov)

• 18536 Cisco IOS Software Crafted Encryption Packet Denial of Service Vulnerability (cisco-sa-20090923-tls)

A Cisco IOS device that is configured for SSLVPN or SSH may reload when it receives a specially crafted TCP packet on TCP port 443 (SSLVPN) or TCP port 22 (SSH). Completion of the three-way handshake to the associated TCP port number of these features is required for the vulnerability to be successfully exploited; however, authentication is not required. A Cisco IOS device that is configured for IKE encrypted nonces may reload when it receives a specially crafted UDP packet on port 500 or 4500 (if configured for NAT Traversal (NAT-T)).

This vulnerability is documented in Cisco bug ID CSCsq24002.

Test Case Impact: **Gather Info** Vulnerability Impact: **DoS / Crash** Risk: **High**

References:

* CONFIRM:
<http://tools.cisco.com/security/center/viewAlert.x?alertId=18892>
* CISCO: 20090923 Cisco IOS Software Crafted Encryption Packet Denial of Service Vulnerability
http://www.cisco.com/en/US/products/products_security_advisory09186a0080af811c.shtml
* SECTRAK: 1022930
<http://www.securitytracker.com/id?1022930>
* VUPEN: ADV-2009-2759
<http://www.vupen.com/english/advisories/2009/2759>

CVE Reference:

CVE-2009-2871 (cve.mitre.org, nvd.nist.gov)

• 18537 Cisco IOS Software Session Initiation Protocol Denial of Service Vulnerability (cisco-sa-20090923-sip)

SIP is a popular signaling protocol that is used to manage voice and video calls across IP networks such as the Internet. SIP is responsible for handling all aspects of call setup and termination. Voice and video are the most popular types of sessions that SIP handles, but the protocol has the flexibility to accommodate other applications that require call setup and termination. SIP call signaling can use UDP (port 5060), TCP (port 5060), or TLS (TCP port 5061) as the underlying transport protocol.

The Cisco Unified Border Element (previously known as the Cisco Multiservice IP-to-IP Gateway) is a special Cisco IOS Software image that runs on Cisco multiservice gateway platforms. It provides a network-to-network interface point for billing, security, call admission control, quality of service, and signaling interworking.

A DoS vulnerability exists in the SIP implementation in Cisco IOS Software when devices are running a Cisco IOS image that contains the Cisco Unified Border Element feature. This vulnerability is triggered by processing a series of crafted SIP messages.

This vulnerability is documented in Cisco Bug ID CSCsx25880.

Test Case Impact: **Gather Info** Vulnerability Impact: **DoS / Crash** Risk: **High**

References:

* CONFIRM:
<http://tools.cisco.com/security/center/viewAlert.x?alertId=18891>
* CISCO: 20090923 Cisco IOS Software Session Initiation Protocol Denial of Service Vulnerability
http://www.cisco.com/en/US/products/products_security_advisory09186a0080af811b.shtml
* SECTRAK: 1022930

<http://www.securitytracker.com/id?1022930>

* VUPEN: ADV-2009-2759

<http://www.vupen.com/english/advisories/2009/2759>

CVE Reference:

CVE-2009-2870 (cve.mitre.org, nvd.nist.gov)

• 18538 Cisco IOS Software H.323 Denial of Service Vulnerability (cisco-sa-20090923-h323)

H.323 is the ITU standard for real-time multimedia communications and conferencing over packet-based (IP) networks. A subset of the H.323 standard is H.225.0, a standard used for call signalling protocols and media stream packetization over IP networks.

The H.323 implementation in Cisco IOS Software contains a vulnerability. An attacker can exploit this vulnerability remotely by sending an H.323 crafted packet to the affected device that is running Cisco IOS Software. A TCP three-way handshake is needed to exploit this vulnerability.

This vulnerability is documented in Cisco bug ID CSCsz38104.

Test Case Impact: **Gather Info** Vulnerability Impact: **DoS / Crash** Risk: **High**

References:

* CONFIRM:

<http://tools.cisco.com/security/center/viewAlert.x?alertId=18885>

* CISCO: 20090923 Cisco IOS Software H.323 Denial of Service Vulnerability

http://www.cisco.com/en/US/products/products_security_advisory09186a0080af811a.shtml

* BID: 36494

<http://www.securityfocus.com/bid/36494>

* OSVDB: 58337

<http://osvdb.org/58337>

* SECTRAK: 1022930

<http://www.securitytracker.com/id?1022930>

* VUPEN: ADV-2009-2759

<http://www.vupen.com/english/advisories/2009/2759>

* XF: ciscoios-h323-dos(53446)

<http://xforce.iss.net/xforce/xfdb/53446>

CVE Reference:

CVE-2009-2866 (cve.mitre.org, nvd.nist.gov)

• 18539 Cisco IOS Software Object-group Access Control List Bypass Vulnerability (cisco-sa-20090923-acl)

In Cisco IOS Software an object group can contain a single object (such as a single IP address, network, or subnet) or multiple objects (such as a combination of multiple IP addresses, networks, or subnets). In an ACL that is based on an object group, administrators can create a single access control entry (ACE) that uses an object group name instead of creating many ACEs, which each would require a different IP address. A similar object group, such as a protocol port group, can be extended to limit access to a set of applications for a user group to a server group.

Note: The Cisco Catalyst 6500 Object Groups feature for policy-based ACLs (PBACLs) is not affected by this vulnerability.

A vulnerability exists in Cisco IOS Software that could allow an unauthenticated attacker to bypass access control policies when the Object Groups for ACLs feature is used.

Note: The Object Groups for ACLs feature was introduced in Cisco IOS software version 12.4(20)T.

This vulnerability is documented in the following Cisco Bug IDs:

CSCsx07114

CSCsu70214

CSCsw47076

CSCsv48603

CSCsy54122

CSCsu50252

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

References:

* CONFIRM:

<http://tools.cisco.com/security/center/viewAlert.x?alertId=18876>

* CISCO: 20090923 Cisco IOS Software Object-group Access Control List Bypass Vulnerability

http://www.cisco.com/en/US/products/products_security_advisory09186a0080af8119.shtml

* BID: 36495

<http://www.securityfocus.com/bid/36495>

* OSVDB: 58338

<http://osvdb.org/58338>

* SECTRAK: 1022933

<http://www.securitytracker.com/id?1022933>

* VUPEN: ADV-2009-2759

<http://www.vupen.com/english/advisories/2009/2759>

CVE Reference:

CVE-2009-2862 (cve.mitre.org, nvd.nist.gov)

• 18540 Cisco IOS Software Internet Key Exchange Resource Exhaustion Vulnerability (cisco-sa-20090923-ipsec)

IPsec is an IP security feature that provides robust authentication and encryption of IP packets. IKE is a key management protocol standard that is used in conjunction with the IPsec standard.

IKE is a hybrid protocol that implements the Oakley and SKEME key exchanges inside the Internet Security Association and Key Management Protocol (ISAKMP) framework. (ISAKMP, Oakley, and SKEME are security protocols that are implemented by IKE.).

A vulnerability exists in the IKE implementation of Cisco IOS Software, if the certificate based authentication method is used. Successful exploitation of this vulnerability may result in the allocation of all available Phase 1 SAs, which may prevent new IPSec sessions from being established.

This vulnerability is addressed by the Cisco Bug IDs CSCsy07555 and CSCee72997.

Test Case Impact: **Gather Info** Vulnerability Impact: **DoS / Crash** Risk: **High**

References:

* CONFIRM:

<http://tools.cisco.com/security/center/viewAlert.x?alertId=18887>

* CISCO: 20090923 Cisco IOS Software Internet Key Exchange Resource Exhaustion Vulnerability

http://www.cisco.com/en/US/products/products_security_advisory09186a0080af8117.shtml

* VUPEN: ADV-2009-2759

<http://www.vupen.com/english/advisories/2009/2759>

CVE Reference:

CVE-2009-2868 (cve.mitre.org, nvd.nist.gov)

• 18541 TCP State Manipulation Denial of Service Vulnerabilities in Multiple Cisco Products (cisco-sa-20090908-tcp24) (CVE-2008-4609)

Multiple Cisco products are affected by denial of service (DoS) vulnerabilities that manipulate the state of Transmission Control Protocol (TCP) connections. By manipulating the state of a TCP connection, an attacker could force the TCP connection to remain in a long-lived state, possibly indefinitely. If enough TCP connections are forced into a long-lived or indefinite state, resources on a system under attack may be consumed, preventing new TCP connections from being accepted. In some cases, a system reboot may be necessary to recover normal system operation. To exploit these vulnerabilities, an attacker must be able to complete a TCP three-way handshake with a vulnerable system.

The vulnerabilities for Cisco IOS Software are documented in Cisco Bug ID CSCsv04836.

Test Case Impact: **Gather Info** Vulnerability Impact: **DoS / Crash** Risk: **High**

References:

* MLIST: [dailydave] 20081002 TCP Resource Exhaustion DoS Attack Speculation

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

* MISC:

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

* MISC:

<http://insecure.org/stf/tcp-dos-attack-explained.html>

* MISC:

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

* MISC:

<http://www.cpni.gov.uk/Docs/tn-03-09-security-assessment-TCP.pdf>

* MISC:

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

* MISC:

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

* CISCO: 20081017 Cisco Response to Outpost24 TCP State Table Manipulation Denial of Service Vulnerabilities

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

* CISCO: 20090908 TCP State Manipulation Denial of Service Vulnerabilities in Multiple Cisco Products

http://www.cisco.com/en/US/products/products_security_advisory09186a0080af511d.shtml

* MS: MS09-048

<http://www.microsoft.com/technet/security/Bulletin/MS09-048.msp>

CVE Reference:

CVE-2008-4609 (cve.mitre.org, nvd.nist.gov)

• 18542 Cisco IOS Software Tunnels Vulnerability (cisco-sa-20090923-tunnels) (CVE-2009-2872)

A tunnel protocol encapsulates a wide variety of protocol packet types inside IP tunnels, creating a virtual point-to-point link between internetworking devices over an IP network.

Cisco Express Forwarding is a Layer 3 IP switching technology. It improves network performance and scalability for networks with high and dynamic traffic patterns.

Cisco IOS 12.0 through 12.4, when IP-based tunnels and the Cisco Express Forwarding feature are enabled, allows remote attackers to cause a denial of service (device reload) via a malformed packet that is not properly handled during switching from one tunnel to a second tunnel, aka Bug IDs CSCsh97579 and CSCsq31776.

Test Case Impact: **Gather Info** Vulnerability Impact: **DoS / Crash** Risk: **High**

References:

* CONFIRM:

<http://tools.cisco.com/security/center/viewAlert.x?alertId=18893>

* CONFIRM:

http://www.cisco.com/en/US/products/products_applied_mitigation_bulletin09186a0080af8113.html

* CONFIRM:

http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_sep09.html

* CISCO: 20090923 Cisco IOS Software Tunnels Vulnerability

http://www.cisco.com/en/US/products/products_security_advisory09186a0080af8115.shtml

* OSVDB: 58333

<http://osvdb.org/58333>

* SECTRAK: 1022930

<http://www.securitytracker.com/id?1022930>

* VUPEN: ADV-2009-2759

<http://www.vupen.com/english/advisories/2009/2759>

CVE Reference:

CVE-2009-2872 (cve.mitre.org, nvd.nist.gov)

• 18543 Cisco IOS Software Tunnels Vulnerability (cisco-sa-20090923-tunnels) (CVE-2009-2873)

A tunnel protocol encapsulates a wide variety of protocol packet types inside IP tunnels, creating a virtual point-to-point link between internetworking devices over an IP network.

Cisco Express Forwarding is a Layer 3 IP switching technology. It improves network performance and scalability for networks with high and dynamic traffic patterns.

Cisco IOS 12.0 through 12.4, when IP-based tunnels and the Cisco Express Forwarding feature are enabled, allows remote attackers to cause a denial of service (device reload) via malformed packets, aka Bug ID CSCsx70889.

Test Case Impact: **Gather Info** Vulnerability Impact: **DoS / Crash** Risk: **High**

References:

* CONFIRM:

<http://tools.cisco.com/security/center/viewAlert.x?alertId=18895>

* CONFIRM:

http://www.cisco.com/en/US/products/products_applied_mitigation_bulletin09186a0080af8113.html

* CONFIRM:

http://www.cisco.com/web/about/security/intelligence/Cisco_ERP_sep09.html

* CISCO: 20090923 Cisco IOS Software Tunnels Vulnerability
http://www.cisco.com/en/US/products/products_security_advisory09186a0080af8115.shtml
* OSVDB: 58334
<http://osvdb.org/58334>
* SECTRACK: 1022930
<http://www.securitytracker.com/id?1022930>
* VUPEN: ADV-2009-2759
<http://www.vupen.com/english/advisories/2009/2759>

CVE Reference:

CVE-2009-2873 (cve.mitre.org, nvd.nist.gov)

New Vulnerabilities found this Week

• **CVE-2009-3454 Microsoft CVSS 2.0 Score = 6.8**

Microsoft Internet Explorer does not properly handle a '\0' character in a domain name in the subject's Common Name (CN) field of an X.509 certificate, which allows man-in-the-middle attackers to spoof arbitrary SSL servers via a crafted certificate issued by a legitimate Certification Authority, a related issue to CVE-2009-2408.

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

References:

MISC: <http://www.wired.com/threatlevel/2009/07/kaminsky/>

BID: <http://www.securityfocus.com/bid/36475>

MISC: <http://www.networkworld.com/news/2009/091709-microsoft-ie-security-hole.html>

MISC: <http://www.networkworld.com/news/2009/073009-more-holes-found-in-webs.html>

CVE Reference: [CVE-2009-3454](#)

• **CVE-2009-2683 HP CVSS 2.0 Score = 7.1**

Unspecified vulnerability in the Sender module in HP Remote Graphics Software (RGS) 5.1.3 through 5.2.6 allows remote authenticated users to execute arbitrary code via unknown vectors.

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

References:

HP: <http://www.securityfocus.com/archive/1/archive/1/506783/100/0/threaded>

HP: <http://www.securityfocus.com/archive/1/archive/1/506783/100/0/threaded>

CVE Reference: [CVE-2009-2683](#)

• **CVE-2009-2681 HP CVSS 2.0 Score = 6.8**

Unspecified vulnerability in HP ProCurve Identity Driven Manager (IDM) A.02.x through A.02.03 and A.03.x through A.03.00, on Windows Server 2003 with IAS and Windows Server 2008 with NPS, allows local users to gain privileges via unknown vectors.

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

References:

HP: <http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c01798159>

HP: <http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=c01798159>

VUPEN: <http://www.vupen.com/english/advisories/2009/2707>

BID: <http://www.securityfocus.com/bid/36462>

SECTRACK: <http://securitytracker.com/id?1022915>

SECUNIA: <http://secunia.com/advisories/36792>

CVE Reference: [CVE-2009-2681](#)

• **CVE-2009-3473 IBM CVSS 2.0 Score = 10.0**

IBM DB2 9.1 before FP8 does not require the SETSESSIONUSER privilege for the SET SESSION AUTHORIZATION statement, which has unspecified impact and remote attack vectors.

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

References:

BID: <http://www.securityfocus.com/bid/36540>

CONFIRM: <http://www-01.ibm.com/support/docview.wss?uid=swg21403619>

AIXAPAR: <http://www-01.ibm.com/support/docview.wss?uid=swg11Z55883>

SECUNIA: <http://secunia.com/advisories/36890>

CVE Reference: [CVE-2009-3473](#)

• **CVE-2009-3471 IBM CVSS 2.0 Score = 7.5**

IBM DB2 8 before FP18, 9.1 before FP8, and 9.5 before FP4 does not perform the expected drops of certain table functions upon a loss of privileges by the functions' definers, which has unspecified impact and remote attack vectors.

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

References:

BID: <http://www.securityfocus.com/bid/36540>

CONFIRM: <http://www-01.ibm.com/support/docview.wss?uid=swg21403619>

CONFIRM: <http://www-01.ibm.com/support/docview.wss?uid=swg21386689>

SECUNIA: <http://secunia.com/advisories/36890>

CVE Reference: [CVE-2009-3471](#)

• **CVE-2009-3472 IBM CVSS 2.0 Score = 6.5**

IBM DB2 8 before FP18, 9.1 before FP8, and 9.5 before FP4 allows remote authenticated users to bypass intended access restrictions, and update, insert, or delete table rows, via unspecified vectors.

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

References:

BID: <http://www.securityfocus.com/bid/36540>

CONFIRM: <http://www-01.ibm.com/support/docview.wss?uid=swg21403619>

CONFIRM: <http://www-01.ibm.com/support/docview.wss?uid=swg21386689>

SECUNIA: <http://secunia.com/advisories/36890>

CVE Reference: [CVE-2009-3472](#)

• **CVE-2009-2864 Cisco CVSS 2.0 Score = 7.8**

Cisco Unified Communications Manager (aka CUCM, formerly CallManager) 5.x before 5.1(3g), 6.x before 6.1(4), 7.0.x before 7.0(2a)su1, and 7.1.x before 7.1(2) allows remote attackers to cause a denial of service (service restart) via malformed SIP messages, aka Bug ID CSCsz95423. An unauthenticated, remote attacker could exploit this vulnerability to cause the affected application to fail, resulting in a DoS condition.

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

References:

CONFIRM: <http://tools.cisco.com/security/center/viewAlert.x?alertId=18883>

XF: <http://xforce.iss.net/xforce/xfdb/53447>

VUPEN: <http://www.vupen.com/english/advisories/2009/2757>

SECTRAK: <http://www.securitytracker.com/id?1022931>

BID: <http://www.securityfocus.com/bid/36496>

CISCO: http://www.cisco.com/en/US/products/products_security_advisory09186a0080af8118.shtml

SECUNIA: <http://secunia.com/advisories/36836>

OSVDB: <http://osvdb.org/58344>

CVE Reference: [CVE-2009-2864](#)

• **CVE-2009-2866 Cisco CVSS 2.0 Score = 7.8**

Unspecified vulnerability in Cisco IOS 12.2 through 12.4 allows remote attackers to cause a denial of service (device reload) via a crafted H.323 packet, aka Bug ID CSCsz38104.

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

References:

CISCO: http://www.cisco.com/en/US/products/products_security_advisory09186a0080af811a.shtml

CONFIRM: <http://tools.cisco.com/security/center/viewAlert.x?alertId=18885>

XF: <http://xforce.iss.net/xforce/xfdb/53446>

VUPEN: <http://www.vupen.com/english/advisories/2009/2759>

SECTRAK: <http://www.securitytracker.com/id?1022930>

BID: <http://www.securityfocus.com/bid/36494>

OSVDB: <http://osvdb.org/58337>

CVE Reference: [CVE-2009-2866](#)

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