netVigilance

ScoutNews Team

23 January 2004
Issue #4

Weekly ScoutNews by netVigilance

Table of Contents

Top Security News Stories this Week

- **Introducing New Legal Defense To Computer Crime Charges**

  According to Greek mythology, the seer Laocoon, a priest of Apollo, warned the residents of Troy against accepting into their city the giant wooden horse designed by Odysseus and created by the architect Epeius. His famous warning, "Trojans, trust not the horse. Whatever it be, I fear the Greeks, even when bringing gifts," applies equally today to importing unknown files as it did to the Trojans 4,000 years ago. We think we know all about the dangers of Trojan horses, but there is a new and more dangerous legal wrinkle to consider. In the past few months, a couple of people in England were acquitted based upon the so-called "Trojan defense" -- what we criminal lawyers used to call the "SODDI" defense: Some Other Dude Did It.

  The Trojan defense presents two equally frightening problems: the possibilities of acquitting the guilty, or convicting the innocent.

  http://www.securityfocus.com/columnists/208
  By Mark Rasch – Security Focus

- **Spammers Use Copyright Get Hacked By Anti-spammers**

  Habeas, the company known for putting copyrighted haikus in legitimate email to distinguish it from spam, says it has come under attack from an as yet unidentified spammer. The spammer is illegally using the Habeas Warrant Mark in emails which are promoting websites such as pharmawarehouse.biz, pharmacourt.biz and valuepointmeds.biz. The attack began about a week ago. Complaints are returning to Habeas. In the trade, such a forgery is called a Joe Job (and here's why).

  http://www.theregister.co.uk/content/55/34969.html
  By Jan Libbenga – The Register

- **Windows 2000 Security Hardening Guide**

  Published January 21, 2003, this document provides administrator guidance for how to set up and configure secure Windows 2000 systems in several scenarios. This document is a baseline for other hardening guides published by Microsoft, such as the Microsoft Solutions for Security.

This document is not meant as a replacement for the Windows 2000 Common Criteria Security Configuration Guide, but rather as a more generally applicable hardening guide which applies to a much broader range of specific systems which may include or exclude services specified in the Windows 2000 Common Criteria evaluated configuration. The recommendations in this guide were generally chosen to safely allow Microsoft customers to deploy the recommended settings on existing Windows 2000 systems, not just on newly-built systems. We have also reviewed the default permissions on Windows Server 2003 and recommended those permissions here where they did not break existing Windows 2000 Server services.

This guide covers hardening of Windows 2000 in three different configurations each for Windows 2000 Professional and the Windows 2000 Server family. The configurations are designed to be very generic to enhance applicability.

View Online:
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/prodtech/win2000/win2khg/default.asp

Download document:
http://www.microsoft.com/downloads/details.aspx?FamilyID=15E83186-A2C8-4C8F-A9D0-A0201F639A56&DisplayLang=en

Windows 2000 Common Criteria Security Configuration Guide
Overview: Windows 2000 Common Criteria Certification:
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/topics/issues/w2kccwp.asp

Microsoft Solution for Securing Windows 2000 Server:
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/prodtech/win2000/secwin2k/default.asp

Securing Windows 2000 Server:
http://www.microsoft.com/downloads/details.aspx?FamilyId=9964CF42-E236-4D73-AEF4-7B4FDC0A25F6&displaylang=en

Authoritative Security Guidance for the Enterprise:
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bestprac/default.asp

❖ Hacker Breaks Into Dan Rather's Teleprompter During Broadcast -- Newsman Embarrassed

Veteran CBS News anchor Dan Rather became enraged yesterday after discovering, a full 15 minutes into his newscast, that somebody hacked into the computer which controls his on-air teleprompter. Workers on the set of the CBS Evening News noticed something wrong from the start, but were afraid to speak up. Of course, this was merely a spoof. Not a hacking spoof, but a real spoof. With worms and hacking piercing the mainstream consciousness, it was only a matter of time before the humorist got a hold of it too. Read for a bit of levity.

http://www.thespoof.com/news/spoof.cfm?headline=s2i1730
By Doug Powers – The Spoof.com

❖ Bagle Virus: The Next Sobig.F?

A potentially devastating virus emerged last week, threatening to unleash the kind of widespread disruption the PC industry experienced last year with Sobig.F. But the Bagle.a virus, alternatively called Beagle and Bagel, petered out rather quickly this week after infecting hundreds of thousands of computers, according to security experts. The virus is categorized as a mass-mailing virus, which means that it replicates by spreading through email attachments. But Bagle.a might be just the first in a series of related electronic attacks. Keep an eye out for

http://www.winnetmag.com/windowspaulthurrott/Article/ArticleID/41526/windowspaulthurrott_41526.html
By Paul Thurrott – WinInfo Windows and NT Magazine
Click here to read what Symantec has to say about Beagle
Click here to see what Trend Micro has to say about Bagle
Click here to see what Sophos has to say about Bagle
Click here to see what McAfee has to say about Bagle
Click here to see what Computer Associates has to say about Bagle

Hmmmm... it seems that only Symantec called this puppy a Beagle... and everyone else went for Bagle. Which leaves one to wonder if this is yet another virus coder that can't spell... and he probably meant bagel. Either way, this puppy has a short shelf life and all the servers that it tries to report to appear to have been blocked off already... but the anti-virus pros are all proclaiming that this is just a test version for 'something much bigger'.

One of life's little mysteries...

New Vulnerabilities Tested in SecureScout

Six new vulnerability Test Cases have been incorporated into the SecureScout database this week. Of course, these weekly updates are what keeps your network scanning tool one step in front of the hackers, inside or outside the organization.

➢ 14362 CD-ROM Allocation Vulnerability

A Windows NT system does not restrict access to removable media drives such as CD-ROM drive. The CD-ROM is available to all users on the system including network users. For best security practice, the CD-ROM should only be available to the user who is logged on at the console.

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

CVE Link: http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-1999-0594
Microsoft Bulletin: http://support.microsoft.com/support/kb/articles/q172/5/20.asp

➢ 14389 Vulnerability in Microsoft Internet Security and Acceleration Server 2000 H.323 Filter Could Allow Remote Code Execution

A security vulnerability exists in the H.323 filter for Microsoft Internet Security and Acceleration Server 2000 that could allow an attacker to overflow a buffer in the Microsoft Firewall Service in Microsoft Internet Security and Acceleration Server 2000. An attacker who successfully exploited this vulnerability could try to run code of their choice in the security context of the Microsoft Firewall Service. This would give the attacker complete control over the system. The H.323 filter is enabled by default on servers running ISA Server 2000 computers that are installed in integrated or firewall mode.

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

CVE Link: http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2003-0819
Microsoft:
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/ms04-001.asp

- **14390 Unchecked buffer in the Multiple UNC Provider Could Enable Code Execution**

The Multiple UNC Provider (MUP) is a Windows service that assists in locating network resources that are identified via UNC (uniform naming convention). The MUP receives commands containing UNC names from applications and sends the name to each registered UNC provider, LAN Manager workstation, and any others that are installed. When a provider identifies a UNC name as its own, the MUP automatically redirects future instances of that name to that provider.

Test Case Impact: **Gather Info** Vulnerability Impact: **Gain Root** Risk: **Medium**

CVE Link: http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2002-0151
Microsoft:
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS02-017.asp

- **14391 Unchecked Buffer in Windows Shell Could Lead to Code Execution**

An unchecked buffer exists in one of the functions that helps to locate incompletely removed applications on the system. A security vulnerability results because it is possible for a malicious user to mount a buffer overrun attack and attempt to exploit this flaw. A successful attack would have the effect of either causing the Windows Shell to crash, or causing code to run in the user's context.

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

CVE Link: http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2002-0070
Microsoft:
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS02-014.asp

- **17831 QuikStore Shopping Cart Discloses Installation Path**

QuikStore is a Shopping Cart programs. The product has been found to contain a security vulnerability disclosing the true path under which the program has been installed. A remote user can send a request to cause the QuikStore Shopping Cart to display an error message that indicates the installation path.

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

CVE Link: http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2002-1455
Securiteam: http://www.securiteam.com/securitynews/5HP0120BQQ.html

- **17832 QuikStore Shopping Cart Viewing and Executing Arbitrary Files**

QuikStore Shopping Cart allows remote file reading and command execution with the privileges of the web server.

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

CVE Link: No CVE link available
Securiteam: http://www.securiteam.com/securitynews/5HP0120BQQ.html

New Vulnerabilities this Week

SuSE Scripts Use Unsafe Temporary Files and May Allow Local Users to Gain Elevated Privileges
Vulnerabilities were reported in several scripts shipped with SuSE Linux. A local user may be able to gain elevated privileges. Check it out.
For more information, see http://securitytracker.com/alerts/2004/Jan/1008804.html
Source: Security Tracker

Apache mod_perl File Descriptor Leak May Let Local Users Hijack the http and https Services
A vulnerability was reported in mod_perl for the Apache web server. A local user can hijack the Apache http and https services. It's been reported that mod_perl leaks critical file descriptors when running on Apache 2.0.x. A local user can create a Perl CGI application that can cause Apache to leak a descriptor and then can take control of the affected service.
For more information, see http://www.securitytracker.com/alerts/2004/Jan/1008822.html
Source: Security Tracker

ISC BIND 8 Invalid Expiry Time Denial Of Service Vulnerability
A denial of service vulnerability has been reported for ISC BIND 8. The vulnerability is due to caching of SIG RR (resource records) with invalid expiry times. An attacker who controls an authoritative name server may be able to cause vulnerable BIND 8 servers to cache invalid SIG RR elements. When the vulnerable DNS server attempts to reference the SIG RR elements it will result in the denial of service condition. Lots of Operating Systems affected. Check to see if yours is vulnerable.
For more information, see http://www.securityfocus.com/bid/6159/info/
Source: SecurityFocus

GNU Privacy Guard Insecure Trust Path To User ID Weakness
GNU Privacy Guard has been reported prone to weakness involving the validity of multiple user IDs. It has been reported that GNUPG does not sufficiently differentiate between the validity given to individual IDs on a public key that has multiple user IDs linked to it. This may result in the leakage of data presumed to be destined to a trusted user; other attacks may also be possible.

For more information, see http://www.securityfocus.com/bid/7497
Source: Security Focus

'the banner exchange' Input Validation Flaw Lets Remote Authenticated Users Execute Arbitrary Code

A vulnerability was reported in 'the banner exchange' (tbe). A remote authenticated user can execute arbitrary code with the privileges of the web server process. It is reported that the banner creation feature does not validate user-supplied input. The user input is reportedly placed into a file with the following type of file name: /bn/tbe-$user_id-$banner_id.html . A remote authenticated user can reportedly place arbitrary code into the file (such as PHP code). A remote user can then cause the banner to be loaded by viewing it or previewing it, executing the code with the privileges of the web server, according to the report.
For more information, see http://www.securitytracker.com/alerts/2004/Jan/1008823.html
Source: Security Tracker

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.