Skip to site navigation (Press enter)

[INFOCON] - OCIPEP DAILY BRIEF Number: DOB02-071 Date: 30 May2002

Wanja Eric Naef [IWS] Thu, 30 May 2002 11:21:44 -0700

DAILY BRIEF Number: DOB02-071 Date: 30 May 2002

NEWS

OCIPEP Issues Advisory - Buffer Overflow Vulnerability
OCIPEP has issued Advisory AV02-027 to bring attention to a remotely exploitable buffer overflow in Macromedia JRun 3.0 and 3.1, earlier reported by CERT/CC. The vulnerability can permit remote execution of arbitrary code on a system with system privileges.

Comment: The OCIPEP Advisory AV02-027 can be found at:
http://www.ocipep-bpiepc.gc.ca/emergencies/advisories/AV02-027_e.html

Hacker Group Attempts DDoS against NATO
A group calling itself "Stop the NATO" launched a distributed denial-of-service (DDoS) attack against the main web site of the North Atlantic Treaty Organization (NATO) on May 28, according to security firm iDefense. The attack, which coincided with the meeting of NATO leaders at an air force base near Rome, Italy, had not had much effect as of mid-day Wednesday. iDefense believed that very few people had downloaded the Flash tool available on the Stop the NATO web site, and that because the tool was single-threaded, a large number of participants would have to join the "Netstrike Against NATO" campaign for it to disrupt normal operations. (Source: iDefense, 29 May 2002)

Comment: OCIPEP has no information indicating that the attack was successful or resulted in any noticeable degradation of NATO systems

IN BRIEF

Alberta Fire Update
The House River fire burning near the hamlet of Conklin is still out of control, and strong winds in the forecast are going to make the firefighters' task even more difficult, according to a wildfire information officer. People staying in shelters will not be able to return to their homes for a few days yet. (Source: The Globe and Mail, CBC News, 29 May 2002)
http://www.globeandmail.ca/servlet/RTGAMArticleHTMLTemplate/C/20020529/wfire
y0529?hub=
homeBN&tf=tgam%252Frealtime%252Ffullstory.html&cf=tgam/realtime/config-neutr
al&vg=BigAdVariableGenerator&slug=
wfirey0529&date=20020529&archive=

RTGAM&site=Front&ad_page_name=breakingnews
http://edmonton.cbc.ca/template/servlet/View?filename=ck_5282002

Manitoba Forest Fire Threatens Communities
A forest fire raging in northern Manitoba may have been deliberately set, according to fire investigators. The fire was burning near two communities, Powell and Barrows, but as of yesterday the wind was pushing it away from the residential areas. Some residents of Powell were evacuated from their homes on Tuesday, and Barrows residents remained on evacuation alert. (Source: CBC News, 29 May 2002)
http://winnipeg.cbc.ca/template/servlet/View?filename=mb_fires020529

Texas Company Faces Problems with Energy Deregulation
The transfer of customers to new energy service providers caused some difficulties for the Electric Reliability Council of Texas Inc. (ERCOT), prompting it to hire an agency to deal with the problems. Following energy deregulation in Texas, ERCOT became responsible for arranging the supply of electricity to most of the state through new service providers. The agency hired, The Feld Group Inc., will oversee the company's systems upgrade. (Source: Computerworld.com, 27 May 2002)
http://www.computerworld.com/managementtopics/management/outsourcing/story/0,10801,71495,00.html

Comment: The ERCOT is unique in the North American Electric Reliability Council (NERC) in that its mandate is limited to one state. This gave ERCOT an unprecedented opportunity to play a key role in the deregulation of the electricity market in Texas.

NORAD to Oversee No-Fly Zone for G8 Summit
CF-18 fighter jets, under the command of North American Aerospace Defense Command (NORAD), will be patrolling the skies over Kananaskis during the June 26-27 G8 Summit. Security measures at the Summit will be more stringent than those put in place during the Winter Olympics in Salt Lake City, according to Major Doug Martin, Deputy Director of Public Affairs at NORAD. Planes flying over the Summit site will be diverted away from Kananaskis. (Source: CBC News, 29 May 2002)
http://calgary.cbc.ca/template/servlet/View?filename=jt_5292002

FBI Announces Major Changes in Organization
The FBI will hire hundreds of agents and update its computer systems in order to adapt to current priorities, particularly the fight against terrorism. FBI Director Robert Mueller announced on Wednesday the creation of a new Office of Intelligence that will concern itself with the prevention of terrorist attacks. Another new division will focus on cyber crime and include parts of the National Infrastructure Protection Center (NIPC). (Source: govexec.com, 29 May 2002)
http://www.govexec.com/dailyfed/0502/052902t1.htm

Stolen Cyanide Containers Found in Mexico
A Mexican police officer found 70 of the 96 drums of sodium cyanide that had been reported missing. The truck carrying them was stolen on May 10, and 20 of the drums were found along with the abandoned truck a week later. State and local officials have given varying numbers for the drums found, which indicates that some of the stolen cyanide could still be missing. (Source: The Nando Times, 29 May 2002)
http://www.nandotimes.com/special_reports/terrorism/investigation/story/417658p-3330368c.html

CYBER UPDATES
See: What's New for the latest Alerts, Advisories and Information Products

Threats

Trend Micro reports on VBS_PLEXIS.A, which is a nondestructive virus that infects MS Word and Excel files using MAPI to send e-mail with PE_PLEXIS.A as an attachment to everyone in the victim's address book.
http://www.antivirus.com/vinfo/virusencyclo/default5.asp?VName=VBS_PLEXIS.A

McAfee Security reports on W32/Enemany.b@MM, which is a worm written in Visual Basic that propagates via MS Outlook e-mail with the subject "Edonkey Update" and the attachment "Esel_Update.Exe".
http://vil.nai.com/vil/content/v_99509.htm

McAfee Security reports on W32/Enemany.a.intd, which is an intended mass-mailing worm but messages sent by this worm do not contain the intended attachment due to a typo in the code. It arrives with the subject "The New Xerox Update for our WinXP"
http://vil.nai.com/vil/content/v_99508.htm

Vulnerabilities

SecurityFocus reports on a buffer overflow vulnerability in MS Active Data Objects (ADO). View the "solution" tab for workaround information.
http://online.securityfocus.com/bid/4849/discussion/

SecurityFocus reports on multiple vulnerabilities in MS SQL Server 2000 including heap and stack based buffer overflows and network denial-of-services attacks. No known patch is available as of yet.
http://online.securityfocus.com/bid/4847/discussion/

SecurityFocus reports on a heap overflow vulnerability in MS IIS 5.0's HTR ISAPI extension that could result in a denial-of-service or allow a remote attacker to execute arbitrary instructions on the victim host. No known patch is available as of yet.
http://online.securityfocus.com/bid/4855/discussion/
http://online.securityfocus.com/bid/4846/discussion/

SecurityFocus reports on a buffer overflow vulnerability in MS Windows 2000's Remote Access Service (RAS). No known patch is available as of yet.
http://online.securityfocus.com/bid/4852/discussion/

SecurityFocus reports on a vulnerability in HTML Help ActiveX control (Hhctrl.ocx), which ships as part of MS HTML Help and can be used to exploit denial-of-service attacks and stack and heap based overflow attacks. View "solution" tab for workaround information.
http://online.securityfocus.com/bid/4857/discussion/

SecurityFocus reports on multiple buffer overflow vulnerabilities in MS Commerce Server 2000 that could allow a remote attacker to execute arbitrary

attacker-supplied instructions with the privileges of the MS Commerce Server 2000 process. No known patch is available as of yet.
http://online.securityfocus.com/bid/4853/discussion/

SecurityFocus reports on buffer overflow vulnerabilities in Oracle Reports Server, Oracle Web Cache and Oracle TNSListener that could allow a remote attacker to execute code on a vulnerable system, access the local system, and gain the privileges of the relevant process. View the "solution" tab for workaround information.
http://online.securityfocus.com/bid/4848/discussion/
http://online.securityfocus.com/bid/4856/discussion/
http://online.securityfocus.com/bid/4845/discussion/

SecurityFocus reports on a format string vulnerability in Oracle Application Server that could allow a remote attacker to write data to arbitrary addresses in memory, and to potentially execute arbitrary code. No known patch is available as of yet.
http://online.securityfocus.com/bid/4844/discussion/

SecurityFocus reports on a vulnerability in phpBB2 that could allow a remote attacker to inject script code into forum messages. phpBB versions prior to the phpBB2 series may also be affected. View the "solution" tab for upgrade information.
http://online.securityfocus.com/bid/4858/discussion/

SecurityFocus provides a report on a vulnerability in Novell Netware 5.0 that could allow a remote attacker to discover the location of the webroot. Follow link for solution.
http://online.securityfocus.com/advisories/4157
http://online.securityfocus.com/advisories/4158

SecurityFocus reports on a stack-based overflow vulnerability in Sun Microsystems' iPlanet Webserver that could allow a remote attacker to execute arbitrary code on, and gain control of, iPlanet hosts. Sending data not specially constructed to execute code could cause the server to crash. No known patch is available as of yet.
http://online.securityfocus.com/bid/4851/discussion/

SecurityFocus reports on a buffer overflow vulnerability in Ipswitch WS_FTP Pro for MS Windows. No known patch is available as of yet.
http://online.securityfocus.com/bid/4850/discussion/

SecurityFocus provides a report on a buffer overflow vulnerability in the SuSE tcpdump program that could lead to a root compromise of the vulnerable system. Follow link for upgrade information.
http://online.securityfocus.com/advisories/4156

SecurityFocus provides a report on a vulnerability in Linux-Mandrake fetchmail prior to v5.9.10 that could allow a malicious server to make the fetchmail process write data outside of the array bounds. Follow link for upgrade information.
http://online.securityfocus.com/advisories/4153

SecurityFocus reports on a vulnerability in Opera 6.01/6.02 related to the handling of the 'file' HTML input-type that could allow a malicious attacker to obtain arbitrary files from client systems. View the "solution" tab for upgrade information.
http://online.securityfocus.com/bid/4834/discussion/

SecurityFocus reports on buffer overflow vulnerabilities in the AMANDA amcheck component and amindexd daemon that could allow a local attacker to execute arbitrary instructions as root. View the "solution" tab for upgrade information.
http://online.securityfocus.com/bid/4840/discussion/
http://online.securityfocus.com/bid/4836/discussion/

SecurityFocus reports on a vulnerability in Falcon Web Server for MS Windows, which may disclose known password protected files that reside on the webserver to unauthorized users. No known patch is available as of yet.
http://online.securityfocus.com/bid/4833/discussion/

SecurityFocus provides a report on a vulnerability in the OpenServer 5.0.5 OpenServer 5.0.6 sort and scoadmin commands, which creates and uses temporary files insecurely allowing names to be predicted and spoofed with symbolic links. Follow link for upgrade information.
http://online.securityfocus.com/advisories/4154
http://online.securityfocus.com/advisories/4155

SecurityFocus reports on a vulnerability in Transoft Broker, which is an FTP server for Windows, that could allow FTP users to cause the host to stop responding. No known patch is available as of yet.
http://online.securityfocus.com/bid/4864/discussion/

SecurityFocus reports on a buffer overflow vulnerability in DataWizard FtpXQ that could result in a denial-of-service. It may also be possible for attackers to execute arbitrary code on target servers. No known patch is available as of yet.
http://online.securityfocus.com/bid/4862/discussion/

SecurityFocus reports on multiple buffer overflow vulnerabilities in Tomahawk Technologies Inc.'s SteelArrow Web Application Server that could allow a remote attacker to execute arbitrary code on a target host. No known patch is available as of yet.
http://online.securityfocus.com/bid/4860/discussion/

SecurityFocus reports on a vulnerability in WoltLab Burning Board that makes it possible to hijack an account that has not yet been activated. View the "solution" tab for workaround information.
http://online.securityfocus.com/bid/4859/discussion/

Tools
There are no updates to report at this time.

CONTACT US

For additions to, or removals from the distribution list for this product,
or to report a change in contact information, please send to:
Email:

For urgent matters or to report any incidents, please contact OCIPEP's
Emergency Operations Centre at:

Phone: (613) 991-7000
Fax: (613) 996-0995
Secure Fax: (613) 991-7094
Email:

For general information, please contact OCIPEP's Communications Division at:

Phone: (613) 991-7035 or 1-800-830-3118
Fax: (613) 998-9589
Email:
Web Site: www.ocipep-bpiepc.gc.ca

Disclaimer
The information in the OCIPEP Daily Brief has been drawn from a variety of
external sources. Although OCIPEP makes reasonable efforts to ensure the
accuracy, currency and reliability of the content, OCIPEP does not offer any
guarantee in that regard. The links provided are solely for the convenience
of OCIPEP Daily Brief users. OCIPEP is not responsible for the information
found through these links.

Navigate to other messages

- Previous message
- View by thread
- View by date
- Next message

Navigate to other messages within this thread

Reply via email to

Wanja Eric Naef [IWS]