

Internationally renowned

Mihai Moldovanu: Ramen worm analysis

zdnet.com

ZDNet Australia
Where technology means business

ADSL2+ WITH VOIP

\$49.99 PER MONTH
MIN CHARGE \$19.82

News Videos Blogs Insight Reviews Whitepapers Downloads iPhone

Search ZDNet Australia News

Hardware Software Security Communications Business Archive

News > Security

Net worm attacks Linux servers

Robert Lemos, ZDNet News
18 January 2001 10:28 AM
Tags: hacking, linux, worm, servers, spread

An Internet worm cobbled together from generally available hacking tools has compromised hundreds, perhaps thousands, of Linux servers. It uses two well-known security flaws in applications set up during the default installation of Red Hat Linux software.

Known as the Ramen worm, the self-spreading program appears to have been created by common Internet vandals - called script kiddies. As of last night, the worm was continuing to spread.

"This is not a very dangerous worm," said Lance Spitzner, coordinator for the HoneyNet Project, a group of well-known security experts who study how hackers attack servers. "It has a very big signature. It is easy to find. And it doesn't really do anything destructive."

The worm spreads by scanning the Internet for servers based on Red Hat 6.2 or 7.0 and then attempts to gain access using two common exploits. When it does gain access, it installs a so-called "root kit," which patches the security holes and installs special programs that replace common system functions. Ramen also replaces the main page on Web servers with an HTML file claiming: "Ramen Crew -- Hackers loooooooooooooooooooooo noodles."

Finally, the new worm sends an email message to two Web-based accounts, boots up and starts scanning the Internet again.

Worm spreading rapidly
Spitzner and other security experts on the Bugtraq mailing list detected the worm earlier this week when they noticed an increase in scans for the RPC.statd and wu-FTP vulnerabilities that plague the default installations of most Linux servers. The worm, however, limits its spread to servers based on Red Hat 6.2 and 7.0.

RPC.statd is one of several services that a Linux server can run to offer remote access using a common suite of programs known as remote procedure calls. Washington University's version of the common file server, known as wu-FTP, has a flaw that also allows access. Patches for both flaws are readily available.

Just In Most Popular Most Discussed

- DBCDE official: NBN a \$43bn question mark
- IIA wants in on iNet piracy case
- Telstra's Thodey just a "nicer face": Optus
- Govt seeks advice on gateways
- Vodafone backs away from 2G advice
- Still no arrests from AFP raid
- CITEC swallows Qld's transformation project
- Curtin Uni picks Microsoft Live@edu
- Doug Campbell: Video interview
- Telstra kills nowwearetalking site

Tip us off:

LOGIN

E-mail

Password (forget?)

Login Remember

Like 124,000 other people join the community and get the latest news from the IT industry.

Join Now

advertisement

TECH SHOWCASE

Cutting-edge technology from premium sponsors

Polycom Voice Solutions

Communications for the way you work

Find the right phones to meet your business communications needs

Conroy's internet filter is a giant funnel
With apologies to John Clarke and Bryan Dawe, ZDNet.com.au's Ratings team has put together its own interpretat... Watch it now

Outlook 2010 technical preview
Microsoft's workhorse Outlook program gets an update in the 2010 suite, but is it enough to upgrade? ... Watch it now

Opera 10
What's new in the Opera 10 browser? Oh, just a major compression engine, better customisations and dual-ident... Watch it now

cnet.com

home | reviews | news | downloads | cnet tv | On TechRepublic: Do video games make you fat & depressed? | log in | join CNET

cnet news

Latest News Crave Webware Business Tech Green Tech Wireless Security Photos More

Home > News > Business Tech

January 17, 2001 12:35 PM PST

Internet worm squirms into Linux servers

By Robert Lemos
Staff Writer, CNET News

Post a comment

Related Stories

- Antivirus firm says Shockwave virus spreading quickly
December 1, 2000
- Experts say Linux attacks not unusual
December 1, 1998

An Internet worm cobbled together from generally available hacking tools could swamp infected portions of the Net with its high-bandwidth searches for vulnerable servers, researchers said Wednesday.

Known as the Ramen worm, the self-spreading program appears to have been created by common Internet vandals--called script kiddies--and limits itself to infecting Red Hat servers that haven't been secured properly.

"The worm itself seems dangerous due to bandwidth consumption and due to the (unproven) possibility of remotely accessing the compromised box by the worm author," said Mihai Moldovanu, a Romanian network administrator for Radio ProFM Bucharest, who reverse-engineered much of the worm Tuesday.

"Once the worm starts scanning, it will consume a large amount of your Internet bandwidth," said the programmer. "The scanning is very fast."

According to Moldovanu, the worm scanned two B-class networks--about 130,000 Internet addresses--in less than 15 minutes. As of Wednesday afternoon, the worm continued to spread.

Lax security to blame
The worm exploits several well-known flaws on Linux servers based on the default installation of versions 6.2 and 7.0 of Red Hat's distribution of Linux.

"It's a lack of awareness," said Lance Spitzner, coordinator for the HoneyNet Project, a group of well-known security experts who study how hackers attack servers. "Not enough people are taking measures to secure the default installations.

"Most default installations are insecure," he stressed.

Spitzner, Moldovanu and other security experts on SecurityFocus.com's Incidents mailing list detected the worm earlier this week when they noticed an increase in scans for two common flaws that plague the default installations of most Linux servers.

Sponsored Links

- CDMA 3G Mobile Info**
Your Technology Intelligence Agent Get Latest Updates From IT Field!
www.itbusinessedge.com
- The Power of a Cell Phone**
Global penetration of mobile phones and new ways for people to connect
www.america.gov
- Unlock/Jailbreak Phone**
Unlock Phone 2G, 3G & 3Gs 3.0 Fast, Easy & Secure for only \$19.99
www.unlock-iphone.us

Most Popular

- Google's mystery UFO doodle finally explained
- Apple offers sleek cachet for clunkers
- Google's gourmet embarrassed on 'Top Chef'
- Psychologist: Facebook makes you smarter, Twitter makes you dumber

Latest tech news headlines

- Join us for Apple's 09/09/09 event
Posted in News - Apple by Erica Ogg
September 8, 2009 11:30 AM PDT
- Final Fantasy XIII Japan launch announced
Posted in The Digital Home by Don Reisinger
September 8, 2009 11:30 AM PDT

Internationally renowned

Liviu Andreicut: IBM Best Linux Application

Bizcity.ro

adevarul.ro

PLUS: premium content din **Biz** BUSINESS REVIEW

BizCity.ro

HOME | EVENIMENT | COMPANII | FINANTE | PIATA DE CAPITAL | IT & C | IMOBILIARE | MARKETING | MANAGEMENT

Miercuri 09.09.2009 ora 15:00 Newsletter | Anunturi imobiliare | Contact | Revista Biz



Home » IT & C » Un student roman premiat de IBM

Un student roman premiat de IBM

24 Martie 2003

comenteaza | recomanda | print

Douazeci de studenti din lumea intreaga, printre care si un **roman**, au castigat cea de-a doua editie a IBM Linux Scholar Challenge, anunta un comunicat al companiei. La categoria universitati a iesit castigator Institutul Indian pentru Tehnologie din New Delhi, care s-a situat pe primul loc intre cele 646 universitati din 68 tari participante. Dintre cei 2.871 studenti care au participat la concurs au fost desemnati 20 de castigatori individuali care primesc sisteme **laptop** IBM ThinkPadR cu sistem de operare Linux. Printre premiantii individuali se afla si Andreicut Liviu de la Universitatea Politehnica din **Bucuresti**, care a participat la competitia mondiala cu un proiect de imbunatatire a functionalitatii consolei, "Improving Console functionality". Dintre cei 20 de castigatori, trei vor primi stagii de pregatire in **vara** lui 2003 la IBM Linux Technology Center, unde vor avea ocazia sa lucreze la proiecte IBM Linux in laboratorul IBM dedicat programarii Linux. Rezultatele muncii lor pe perioada stagiului vor fi incorporate in produse si tehnologii IBM Linux care vor dirija urmatoarea etapa de **e-business**. (Ana Maria Florea)

adevărul.ro „Adevărul”

9 septembrie 2009 | Arhiva | RSS | Versiunea Mobil | Publicitate | Abonamente | English Version

HOME | ACTUALITATE | SPORT | FINANCIAR | INTERNAȚIONAL | SOCIETATE

Pe scurt

Data: 1 apr 2003
21 afișări

Mărime text: Trmite unui prieten Print

IBM Linux Scholar Challenge are printre castigatori si un student din Romania

IBM a anuntat recent castigatorii celei de a doua editii a competitiei IBM Linux Scholar Challenge, castigatoarele fiind Indian Institute of Technology (IIT) din Delhi, India. Printre cei 20 de studenti castigatori se afla si Andreicut Liviu de la Universitatea Politehnica din Bucuresti. IIT s-a situat pe primul loc intre cele 646 universitati din 68 tari participante si a primit ca premiu un claster Linux 16-node IBM eServerT xSeriesT. Dintre cei 2.871 studenti care au participat la concurs au fost desemnati 20 de castigatori individuali care primesc sisteme laptop IBM ThinkPadR cu sistem de operare Linux. Printre premiantii individuali se afla si Andreicut Liviu de la Universitatea Politehnica din Bucuresti care a participat la competitia mondiala cu un proiect de imbunatatire a functionalitatii consolei: Improving Console functionality.

Chic parizian la Oltenița!

„Isabella ma belle”, un salon de frumusețe din urbea de pe malul Dunării, are nu numai nume ci și produse pariziene. „Vopseaua de păr folosită aici”, a declarat Isabela Popescu, „este cumpărată direct de la furnizorul exclusiv din Paris, în fiecare lună. Poate părea o fiță să folosim vopsea de păr făcută din filé des escargots și champagne rosé”, mărturisește coafeza. „dar este o afacere ecologică și la îndemână.” Ea a mai spus că este „simplu și accesibil să ne dotăm cu cele mai bune produse din străinătate”. Practic, Isabela trimite bani surorii ei stabilite în Franța, iar aceasta îi cumpără și trimite apoi produsele în țară.

„Acum beneficiazi de reducere când trimiți pentru prima dată bani în străinătate”, explică Isabela. Cum? E simplu: trimite seria și numărul de CI. CI de lungă ședere sau pașaport prin SMS la 1856 sau completează pe www.transferdebani.ro, arată-i operatorului Western Union codul unic primit și vei primi 3 euro reducere. Perioada promoției este august - decembrie 2009.

Fast response time to security issues

Clamav

Clamav 0.88.4 . Problem: remote code execution
Problem fixed in TFM: 8 August 2006
Problem fixed in Suse: 9 August 2006

TFM

```
120
121 %{_libdir}/libclamav.*
122 %{_includedir}/clamav.h
123 %{_bindir}/*clamscan
124 %{_bindir}/*clamdscan
125 %{_bindir}/*freshclam
126 %{_bindir}/*sigtool
127 %{_bindir}/clamav-config
128 /usr/bin/clamav-config
129 %{_sbindir}/*clamd
130 %{_mandir}/man/*
131 %defattr(-, clamav, clamav)
132 %dir /var/spool/clamav/
133 %attr(-,clamav,clamav) %config(noreplace) /var/spool/clamav/main.cvd
134 %attr(-,clamav,clamav) %config(noreplace) /var/spool/clamav/daily.cvd
135 %attr(-,clamav,clamav) %config(noreplace) /var/log/clamd.log
136 %attr(-,clamav,clamav) %config(noreplace) /var/log/freshclam.log
137 # /etc/clamav/clamav.conf
138 %config(noreplace) /etc/clamav/clamd.conf
139 /usr/lib/pkgconfig/libclamav.pc
140 %config(noreplace) /etc/clamav/freshclam.conf
141 /etc/cron.hourly/update-clamav
142 /etc/rc.d/services/rc.clamav
143 /etc/logrotate.d/clamd
144 /etc/logrotate.d/freshclam
145
146 %changelog
147 * Tue Aug 08 2006 Team TFM <pack@tfm.ro> - miham
148 - 0.88.4
149 - Autorestarting on upgrade ( if needed )
```

SUSE

```
-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA1

-----
SUSE Security Announcement

Package: clamav
Announcement ID: SUSE-SA:2006:046
Date: Wed, 09 Aug 2006 16:00:00 +0000
Affected Products: SUSE LINUX 10.1
                   SUSE LINUX 10.0
                   SUSE LINUX 9.3
                   SUSE LINUX 9.2
                   SUSE SLES 10
                   SUSE SLES 9

Vulnerability Type: remote code execution
Severity (1-10): 5
SUSE Default Package: no
Cross-References: CVE-2006-4018

Content of This Advisory:
1) Security Vulnerability Resolved:
   clamav heap buffer overflow
   Problem Description
2) Solution or Work-Around
3) Special Instructions and Notes
4) Package Location and Checksums
5) Pending Vulnerabilities, Solutions, and Work-Arounds:
   - See SUSE Security Summary Report
6) Authenticity Verification and Additional Information
```


Fast response time to security issues

apache

Apache 2.2.12 . Fixed problems: CVE-2009-1891, CVE-2009-1195, CVE-2009-1890
Problem fixed in TFM: 22 July 2009
Problem fixed in Suse: 29 July 2009

TFM

SUSE

The screenshot shows the TFM website interface. At the top, there is a navigation bar with links like 'WIKI', 'Timeline', 'Roadmap', 'Browse Source', 'View Tickets', 'New Ticket', 'Search', and 'Admin'. Below this, the page title is 'root / server / apache2 / trunk / apache2.spec @ 1058'. The main content area displays 'Revision 1058, 11.1 KB (checked in by mihaim, 7 weeks ago)'. A list of changes is shown, including 'kernel, krm update, apache_spr, apr-util updated, httpdmod added' on 2009-07-22T12:24:50+0300 in Timeline. A detailed list of files and their sizes is provided, such as '1. Define contentdir /var/www', '2. Define suexec_caller httpd', '3. Define vstring TFM/SU Linux', and '4. Summary: The most widely used Web server on the Internet'. The page footer includes 'http://dev.tfm.ro/timeLine?from=2009-07-22T12:24:50+0300&precision=second'.

The screenshot shows the SUSE repository index page. At the top, there is a search bar and navigation links. Below this, there is a warning message: 'Aceasta este conținut din memoria cache de la Google pentru http://download.opensuse.org/repositories/home/Phisker/SLES/SLE_10/x86_64/ Este un instantaneu al paginii, așa cum arăta ea în 30 Iul 2009 12:54:44 GMT. Este posibil ca pagina curentă să se fi modificat între timp. [Dați-mi mai multe](#)'. Below the warning, there is a link to 'Sunt evidențiate următorii termeni de căutare: sles apache 2.2.12 rpm' and a link to 'Versiune numal test'. The main content area is titled 'Index of /repositories/home:/Phisker:/SLES/SLE_10/x86_64' and contains a table of files with columns for Name, Last modified, and Size. The table lists various RPM packages such as 'apache-2.2.12-1.i.86_64.rpm', 'apache-debuginfo-2.2.12-1.i.86_64.rpm', 'apache-devel-2.2.12-1.i.86_64.rpm', 'apache-doc-2.2.12-1.i.86_64.rpm', 'apache-event-2.2.12-1.i.86_64.rpm', 'apache-example-certificates-2.2.12-1.i.86_64.rpm', 'apache-example-pages-2.2.12-1.i.86_64.rpm', 'apache-its-2.2.12-1.i.86_64.rpm', 'apache-prefork-2.2.12-1.i.86_64.rpm', 'apache-util-2.2.12-1.i.86_64.rpm', 'apache-worker-2.2.12-1.i.86_64.rpm', 'libapr-util-1.0-122-1.i.86_64.rpm', 'libapr-util-1.3.8-1.2.i.86_64.rpm', 'libapr-util-dbd-mysql-1.3.8-1.2.i.86_64.rpm', 'libapr-util-dbd-pgsql-1.3.8-1.2.i.86_64.rpm', 'libapr-util-dbd-sqlite3-1.3.8-1.2.i.86_64.rpm', 'libapr-util-debuginfo-1.3.8-1.2.i.86_64.rpm', 'libapr-util-devel-1.3.8-1.2.i.86_64.rpm', 'libapr-1.3.7.2-1.i.86_64.rpm', 'libapr-debuginfo-1.3.7.2-1.i.86_64.rpm', 'libapr-devel-1.3.7.2-1.i.86_64.rpm', and 'libaprversion-1.4.6-123-22.i.86_64.rpm'. The page footer includes 'Done' and 'Index of repositories/home:/Phisker:/SLES/SLE_10/x86_64'.