



Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permitted without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials Bootcamp Style (Security 401)"
at <http://www.giac.org/registration/gsec>

Ramen Noodles

Micah Arthur

February 6, 2001

Ramen Noodles, Food for thought....

Its 7:29 AM, and your asleep safe in your bed. You knew about the troubles associated with WU-ftp, but you figured they were not a serious threat. Rising late in the morning, there's no time for breakfast as you dash out the door. There's no need; you have Ramen Noodles waiting for you at the office.

The Ramen worm is a package of well-known exploits for WU-ftp, rpc.statd, and lprng. The purpose of this article is three-fold:

- To detail the usage and spread of the Ramen worm.
- To take a detailed look at the exploitable vulnerabilities.
- Provide an in-depth 'HOW-TO' on vulnerability removal.

Ramen Toolkit/Worm

The Ramen toolkit/worm was added to the CERT website on Thursday, Jan. 18th, 2001. A 'rootkit' in reference to its designed purpose of establishing root access, and a worm in its ability to replicate and seek out new victims. As reported by Robert Lemos on zdnet.com- "Depending on the version of the operating system it's infecting, Ramen can use well-known flaws in Washington University's FTP server software, a component of the Remote Procedure Call services or the printing software LPrng. These programs are normally placed on servers during the default installation of Red Hat 6.2 and 7.0." The most striking piece of information is, "Patches are available for all the flaws used by the worm."

The basic pattern of the exploit runs like this:

- The initial scan is made on port 21 (FTP), and any FTP banners are retrieved. Ramen then uses this banner information to determine if the server is a vulnerable target.
- If the target is vulnerable, a replication script is started and the exploits are launched.
- Using one of the vulnerable services, Ramen creates the /usr/src/.poop directory on the target, and then requests a copy of itself.
- After replicating itself Ramen opens port 27374, and searches out and replaces the target's 'index.html' file.

- It then disables the vulnerable services by which it gained entry, and the target now becomes attacker and seeks out new hosts.

It is worthy of note that this worm currently only targets RedHat installations. Other Linux distributions could be vulnerable as well, but at this time Ramen only targets RedHat systems running 6.2 and 7.0. Even though only RedHat is a target at this time, a few points need to be considered.

1. Ramen is openly available. Variants of the original have and will continue to pop up. If you're running a server with a distribution other than RedHat, you may yet be a target. The same vulnerabilities that Ramen exploits are also native to SuSe, Mandrake, Caldera, and possibly others. As Michael Warfield of ISS explains, "Ramen is currently known to attack Red Hat systems running vulnerable versions of wu-ftp, rpc.statd, and LPRng. New exploits can be added to the existing worm to expand its capabilities."
2. Ramen is a toolkit. It is a package of exploits that have been automated. Each of these exploits can still be run individually without the automation of Ramen.
3. The vulnerabilities that Ramen is searching for were published up to over 4 months ago. The case in point is a clear example of why administrators need to keep abreast of published vulnerabilities. The "script kiddies" are paying attention, even if we are not.

THE VULNERABILITIES

Let us now take a look at the very heart of the Ramen problem, the vulnerabilities that WU-ftpd, rpc.statd, and lprng contain.

WU-ftpd

The Washington University-ftpd software package is one of the more common FTP programs packaged into Linux and BSD distributions. There are two recently reported vulnerabilities in WU-ftpd; the "Site exec" vulnerability, and the "setproctitle()" vulnerability. Of the two, "Site exec" is the one that the Ramen worm is concerned with. The exploit takes advantage of a character-formatting error in the site exec command in versions 2.60 and earlier. To quote CERT, "The wu-ftpd "site exec" vulnerability is the result of missing character-formatting argument in several function calls that implement the "site exec" command functionality. Normally if "site exec" is enabled, a user logged into an ftp server (including the 'ftp' or 'anonymous' user) may execute a restricted subset of quoted commands on the server itself. However, if a malicious user can pass character format strings consisting of carefully constructed *printf() conversion characters (%f, %p, %n, etc) while executing a "site exec" command, the ftp daemon may be tricked into executing arbitrary code as root."

To identify what FTP service is running on your system you can do the following:

- % ftp 'hostname' This should output a banner message that identifies your FTP program.
- If the version number is not displayed, then login to your ftp service and enter, 'quote stat' at the ftp> prompt.
- The vulnerability in discussion resides in WU-ftpd versions 2.60 and earlier.

According to various websites, this vulnerability may have been present for as far back as 1993 and any distributions based off of WU-ftpd are likely to also have this vulnerability. Fortunately, future releases contain the necessary fixes, and for those currently running vulnerable version of WU-ftpd patches are available. RedHat recommends, "If you have not updated your system, we recommend you update these packages immediately." and goes on to offer links to download the appropriate RPMs.

rpc.statd

Ramen also searches for the statd Remote Procedure Call. SecurityFocus.com states that,

"A vulnerability exists in the rpc.statd program which is part of the nfs-utils packages, distributed with a number of popular Linux distributions. Because of a format string vulnerability when calling the syslog() function a malicious remote user can execute code as root. The rpc.statd server is an RPC server that implements the Network Status and Monitor RPC protocol. It's a component of the Network File System (NFS) architecture. The logging code in rpc.statd uses the syslog() function passing it as the format string user supplied data. A malicious user can construct a format string that injects executable code into the process address space and overwrites a function's return address, thus forcing the program to execute the code. rpc.statd requires root privileges for opening its network socket, but fails to drop these privileges later on. Thus code executed by the malicious user will execute with root privileges. Debian, Red Hat and Connectiva have all released advisories on this matter. Presumably, any Linux distribution which runs the statd process is vulnerable, unless patched for the problem."

The basic idea is that rpc.statd is passing user supplied data to syslog as a format string. If there isn't any validation of this string, machine code can be supplied and executed with rpc.statd's privileges- which are usually root. Again, patches pertaining to this vulnerability have been available for some time. By this time, it should becoming painfully obvious to administrators that regular checks need to be performed to see if vulnerabilities have been reported for their running software. Unlike WU-ftpd, the rpc.statd vulnerability leaves behind some excellent clues. CERT placed a detailed description of intruder activity along with their advisory. Consider the following example log message,

For systems without /etc/inetd.conf

- An intruder-supplied program is added as '/usr/sbin/asp'. A service named 'asp' is added to '/etc/xinetd.d' and xinetd is sent a signal to reload it's configuration. This causes xinetd to listen on TCP socket number 27374 for incoming connections.

- The 'lpd' service is terminated

- The system file '/usr/sbin/lpd' is deleted and replaced with an empty file

- Use names 'ftp' and 'anonymous' are added to '/etc/ftpusers'

To detect if your system has been infected, a Ramen detection script has been written by William Stearns and is available at <http://www.sans.org/y2k/ramen.htm>. If you have found that your system has indeed been compromised, there is a very informative section about Ramen removal that can also be found at the above listed Sans.org website.

Stearns, William "Ramen Worm"

Version 0.3 UPDATED 02/05/2001.

<http://www.sans.org/y2k/ramen.htm> (02/06/01)

Houle, Kevin "Widespread Compromises via "ramen" Toolkit"

CERT[®] Incident Note IN-2001-01 01/18/01

http://www.cert.org/incident_notes/IN-2001-01.html (02/06/01)

Evans, Chris "Multiple Vendor LPRng User-Supplied Format String Vulnerability"

Security Focus article on LPRng (from bugtraq) 09/25/01

<http://www.securityfocus.com/bid/1712> (02/06/01)

Lemos, Robert "Net worm hobbles Linux servers"

Ziff Davis online UPDATED 01/23/01

<http://www.zdnet.com/zdnn/stories/news/0,4586,2675147,00.html> (02/06/01)

Lemos, Robert "Vandals mutate Ramen Linux worm"

Ziff Davis online 01/22/01

<http://www.zdnet.com/zdnn/stories/news/0,4586,2677152,00.html> (02/06/01)

Warfield, Michael "Ramen Linux Worm Propagation"

Internet Security Systems Security Alert 01/18/01

<http://xforce.iss.net/alerts/advise71.php> (02/06/01)

Upcoming Training

Click Here to
{Get CERTIFIED!}



| | | | |
|---|-----------------------------|-----------------------------|----------------|
| SANS vLive - SEC401: Security Essentials Bootcamp Style | SEC401 - 201710, | Oct 23, 2017 - Nov 29, 2017 | vLive |
| SANS San Diego 2017 | San Diego, CA | Oct 30, 2017 - Nov 04, 2017 | Live Event |
| San Diego Fall 2017 - SEC401: Security Essentials Bootcamp Style | San Diego, CA | Oct 30, 2017 - Nov 04, 2017 | vLive |
| SANS Seattle 2017 | Seattle, WA | Oct 30, 2017 - Nov 04, 2017 | Live Event |
| SANS Gulf Region 2017 | Dubai, United Arab Emirates | Nov 04, 2017 - Nov 16, 2017 | Live Event |
| Community SANS Vancouver SEC401^ | Vancouver, BC | Nov 06, 2017 - Nov 11, 2017 | Community SANS |
| Community SANS Colorado Springs SEC401~ | Colorado Springs, CO | Nov 06, 2017 - Nov 11, 2017 | Community SANS |
| SANS Miami 2017 | Miami, FL | Nov 06, 2017 - Nov 11, 2017 | Live Event |
| SANS Sydney 2017 | Sydney, Australia | Nov 13, 2017 - Nov 25, 2017 | Live Event |
| SANS Paris November 2017 | Paris, France | Nov 13, 2017 - Nov 18, 2017 | Live Event |
| SANS San Francisco Winter 2017 | San Francisco, CA | Nov 27, 2017 - Dec 02, 2017 | Live Event |
| Community SANS St. Louis SEC401 | St Louis, MO | Nov 27, 2017 - Dec 02, 2017 | Community SANS |
| SANS London November 2017 | London, United Kingdom | Nov 27, 2017 - Dec 02, 2017 | Live Event |
| Community SANS Portland SEC401 | Portland, OR | Nov 27, 2017 - Dec 02, 2017 | Community SANS |
| SANS Khobar 2017 | Khobar, Saudi Arabia | Dec 02, 2017 - Dec 07, 2017 | Live Event |
| SANS Munich December 2017 | Munich, Germany | Dec 04, 2017 - Dec 09, 2017 | Live Event |
| Community SANS Ottawa SEC401 | Ottawa, ON | Dec 04, 2017 - Dec 09, 2017 | Community SANS |
| SANS Austin Winter 2017 | Austin, TX | Dec 04, 2017 - Dec 09, 2017 | Live Event |
| SANS Bangalore 2017 | Bangalore, India | Dec 11, 2017 - Dec 16, 2017 | Live Event |
| SANS vLive - SEC401: Security Essentials Bootcamp Style | SEC401 - 201712, | Dec 11, 2017 - Jan 24, 2018 | vLive |
| SANS Cyber Defense Initiative 2017 | Washington, DC | Dec 12, 2017 - Dec 19, 2017 | Live Event |
| SANS Cyber Defense Initiative 2017 - SEC401: Security Essentials Bootcamp Style | Washington, DC | Dec 14, 2017 - Dec 19, 2017 | vLive |
| Community SANS Nashville SEC401^ | Nashville, TN | Jan 08, 2018 - Jan 13, 2018 | Community SANS |
| Community SANS Hawaii SEC401 | Honolulu, HI | Jan 08, 2018 - Jan 13, 2018 | Community SANS |
| SANS Security East 2018 | New Orleans, LA | Jan 08, 2018 - Jan 13, 2018 | Live Event |
| Mentor Session - SEC401 | Memphis, TN | Jan 09, 2018 - Mar 13, 2018 | Mentor |
| Northern VA Winter - Reston 2018 | Reston, VA | Jan 15, 2018 - Jan 20, 2018 | Live Event |
| SANS Amsterdam January 2018 | Amsterdam, Netherlands | Jan 15, 2018 - Jan 20, 2018 | Live Event |
| Mentor Session - SEC401 | Minneapolis, MN | Jan 16, 2018 - Feb 27, 2018 | Mentor |
| SANS Las Vegas 2018 | Las Vegas, NV | Jan 28, 2018 - Feb 02, 2018 | Live Event |
| Las Vegas 2018 - SEC401: Security Essentials Bootcamp Style | Las Vegas, NV | Jan 28, 2018 - Feb 02, 2018 | vLive |