$2.50

MUUGlines

January 1997 Volume 9, Number 5

This Month's Meeting – Red Hat 4.0 Install Demo!

This month's meeting will feature a quick install (a la Galloping Gourmet) and overview of the features of Red Hat's version 4.0 of the Linux system. Want to get up to speed quickly on how to get this working on your system? Come and quiz the experts! Presenting will be Doug Jackson, with assistance and backup by Gilbert Detillieux.

Future Meetings

The following is a tentative outline of meeting topics for upcoming months:

February 11, 1997: A Look at Java
March 11, 1997: Tools for Net Searching
April 8, 1997: Stupid Web Tricks, and other fun stuff
May 13, 1997: (TBA)
June 10, 1997: MUUG Barbecue

Where To Go

Our fifth meeting of this year will be at our regular location, IBM Canada's offices in the TD Centre building at the corner of Portage and Main. We'll be meeting at the lobby on the main floor, and Steve Moffat will take us up to the meeting room just before the meeting starts.

This month's meeting is on December 10th at 7:30 PM. Please arrive before this time for the meeting, as it will take some time for Steve to get people up to the meeting room.

Parking is available either in the parkade behind the TD building (off Albert St.), or in the ground level lot just north of the TD building. Entrance to the lot is from Albert Street, behind the parkade. Either way, parking is $1.25 flat rate for the evening.

Is Linux Trademarked?

Several readers asked Linux Journal about the registered trademark symbol after Linux, in particular after noting the R[registered] symbol after Linux on IDG Books' Linux Secrets, written by Naba Barkakati. The book's cover says: "Linux is a registered trademark of William R. Della Croce, Jr." Is there really a registered trademark on the word Linux?

IDG Books Worldwide, Inc. told Linux Journal that they did a trademark search as they always do when deciding what to put on a book cover, and although surprised to find a registered trademark on Linux, they printed the information resulting from their search. Their intent was in no way to reinforce the registered mark, but to comply with trademark requirements.

In July, 1996, we at LJ tried to contact the person who had filed for the trademark, Mr. William R. Della Croce, Jr., via phone and left a message giving our e-mail address and telephone number. Mr. Della Croce e-mailed back a brief note to us, stating that "LINUX" was proprietary to him and that we would be hearing from his attorney.

We e-mailed Linus Torvalds about the matter. Linus reiterated his determination that Linux remain in common use or be trademarked by some trustworthy organization or individual.

We investigated the trademark, which was registered August 8, 1995, with a first use date of August 2, 1994. Since this date is long after others have used the term "Linux", it seems there are ample grounds to protest this trademark.

In August 1996, Linux Journal and other Linux companies reported that they had received letters from Mr. Della Croce informing them that:

"LINUX(tm) is proprietary. Information about obtaining approval for use and/or making payment for past use may be obtained by writing to the following address:..."

Yggdrasil Computing filed for a trademark on their book title Linux Bible in March 1995. Their trademark was turned down because Linux was already a trademark registered to Mr. Della Croce. Adam says that in March 1996, Yggdrasil Computing filed a letter disputing Della Croce's trademark and showing that Linux was a generic term and that Yggdrasil's use was prior to Della Croce's in any event. Yggdrasil also asked to have the Linux trademark by Della Croce cancelled.

Yggdrasil Computing should hear back by the end of September, 1996.

The trademark office usually doesn't cancel trademarks without separate action taken. It is very likely this fall, after we hear of the result of Yggdrasil Computing's actions, that Linux companies and individuals will band together to fight to return the word Linux back to the Linux community.

(G. Gervaise Davis III, Business and Intellectual Property Lawyer, is fighting the apparent trademarking of Linux on a pro-bono basis, with Workgroup Solutions paying his expenses. Find out more about intellectual property trademark information from the web page at `http://www.iplawyers.com/`.)

Is Linux Trademarked? (Part II)

Petition to Cancel filed against Linux Trademark

Members of the LINUX community have been up in arms during the past six months over the efforts of an individual named William R. Della Croce, Jr. from the Boston area to collect 10% royalties on sales from businesses marketing Linux products. He bases his written demands on a US trademark which he claims to hold on the name "LINUX" for a computer operating system. He, in fact, holds such a registered trademark, based on his claim made under penalty of perjury

that he is the owner and first user of the mark for operating systems, and that he was not aware in 1994 or 1995 of any other person who might claim or be using this name and mark for an operating system. This claim is absurd on its face.

WorkGroup Solutions, Yggdrasil Computing, Linux International, SSC/Linux Journal, and Linus Torvalds have retained an internationally known software industry attorney, G. Gervaise Davis III, of the Davis & Schroeder law firm in Monterey, CA to seek cancelation of this registration on the grounds that it is fraudulent and obtained under false pretenses. Mr. Davis and his firm are handling the case on a vastly reduced fee basis, because of their long standing relationship with the U.S. software industry. Davis was the original attorney for Gary Kildall and Digital Research of CP/M fame in the 1980s.

A Petition to Cancel was in fact filed with the Trademark Trial and Appeals Board in Washington, DC. on November 27, 1996, detailing the improper actions of Della Croce and setting out the true facts with a number of exhibits and attachments. Mr. Davis advises us that we can expect to have further steps taken by TTAB, under their complex procedural rules over the next few months. TTAB will first notify Della Croce of the filing and permit him time to respond, then evidence can be collected and depositions taken, and then the parties can file briefs and other responses. Often these cases take more than a year to be resolved by a TTAB decision.

All of our industry is fully aware that Linus Torvalds developed Linux and that it has become one of the world's most popular operating systems during the past six years. The participants in this proceeding expect the TTAB to cancel the registration, after hearing and seeing the massive evidence demonstrating that Della Croce had no conceivable legal basis for his claim to the mark.

The petition itself is available on the websites of each of the petitioners and Mr. Davis' law firm at http://www.iplawyers.com/. We urge that interested persons read it, and distribute it and this message to all members of the LINUX community so that they will be aware of what is being done about this outrageous trademark claim. We will try to keep everyone posted on developments in the case through user groups and webpages.

Security Vulnerabilities in Red Hat Linux

The following bulletin is one of many regularly published at the CIAC website (http://ciac.llnl.gov/). The CIAC is the U.S. Department of Energy's Computer Incident Advisory Capability. Established in 1989, CIAC provides computer security services to employees and contractors of the Department of Energy.

H-17: cron/crontab Buffer Overrun Vulnerabilities

December 18, 1996 20:00 GMT

PROBLEM: Problems have been identified in cron(8) and crontab(1) programs.

PLATFORM:

All platforms running FreeBSD 1.0, 1.1, 2.1.0, 2.1.5, 2.1.6, 2.1.6.1 and 2.2.

All platforms running RedHat Linux version 4.0.

All releases of NetBSD up to and including 1.2.

DAMAGE: Local users may gain root privileges.

SOLUTION: Install the proper patches and/or use the workarounds provided below.

VULNERABILITY ASSESSMENT: Exploit information involving this vulnerability has been made publicly available.

[Start AUSCERT Advisory]

AA-96.21 AUSCERT Advisory

cron/crontab Buffer Overrun Vulnerabilities

18 December 1996

AUSCERT has received information that vulnerabilities exist in the cron(8) and crontab(1) programs found in the Unix cron package. These vulnerabilities may allow local users to gain root privileges. Exploit information involving these vulnerabilities has been made publicly available.

The vulnerabilities in the cron package affect numerous vendors and platforms. AUSCERT recommends that sites take the steps outlined in section 3 as soon as possible.

This advisory will be updated as more information becomes available.

1. Description

AUSCERT has received information that vulnerabilities exist in the cron(8) and crontab(1) programs. cron(8) executes commands at specified times according to instructions placed in user crontab files. crontab(1) is used to install, remove or list the tables used to drive the cron daemon. Both of these programs are installed by default.

Two unrelated vulnerabilities are known to exist in some versions of the cron package.

1. Command line buffer overrun

Due to insufficient bounds checking on arguments which are supplied by users, it is possible to overwrite the internal stack space of the crontab program while it is executing. By supplying a carefully designed argument to the crontab program, intruders may be able to force crontab to execute arbitrary commands. As crontab is setuid root, this may allow intruders to run arbitrary commands with root privileges.

2. Reading environment buffer overrun

A similar vulnerability exists in the library routine used to load environment variables. This vulnerable routine is used in both cron and crontab. Due to insufficient bounds checking, it may be possible for intruders to manipulate cron or crontab into executing arbitrary com-

mands with root privileges.

Both of these vulnerabilities are known to be present in the Vixie cron package, up to and including version 3.0. This package is installed by default under some versions of Unix. The Vixie cron package may have also been installed as third party software by sites.

The following command may be used to indicate whether a version of cron based on Vixie cron is installed:

```
# strings /usr/bin/crontab | grep -i vix
```

Sites which have versions based on Vixie cron should consider themselves vulnerable unless they have specific information from their vendors which suggests otherwise.

Other versions of the cron package supplied by vendors may also be vulnerable (Section 3).

Exploit information involving these vulnerabilities has been made publicly available.

2. Impact

Local users may gain root privileges.

3. Workarounds/Solution

AUSCERT recommends that sites limit the possible exploitation of these vulnerabilities by immediately removing the setuid permissions on crontab(1) and checking the contents of crontab files as stated in Section 3.1.

Vendor information about the vulnerabilities described in this advisory is provided in Section 3.2.

If the cron functionality is required for non privileged users, and no vendor information or patches are available (Section 3.2), AUSCERT recommends that access be restricted to a trusted set of users as given in Section 3.3.

3.1 Remove setuid and non-root execute permissions and check crontab files

AUSCERT recommends that the setuid permissions be removed from the crontab program immediately. As the crontab program will no longer work for non-root users, it is recommended that the execute permissions also be removed. For example:

```
# ls -l /usr/bin/crontab
-r-sr-xr-x  1 root    bin    20480 Jun 10
1996 /usr/bin/crontab
# chmod 500 /usr/bin/crontab
# ls -l /usr/bin/crontab
-r-x------  1 root    bin    20480 Jun 10
1996 /usr/bin/crontab
```

Note that this will remove the ability for any non-root user to run the crontab program. This will prevent further exploitation of the crontab vulnerabilities described in this advisory.

In addition, to ensure that cron can not be exploited through existing user crontab files, sites should check the contents of all existing crontab files for unusual contents. Unusual contents may include very long lines or lines containing non-ASCII characters. If strange environment settings or other unusual entries are found, it may indicate a possible attack. User crontab files are usually located in either /var/cron/tabs or /var/spool/cron.

3.2 Vendor information

Below is a list of vendors which are known to be affected by the crontab vulnerabilities described in this advisory:

RedHat Linux
FreeBSD, Inc
NetBSD Project

The following vendors have informed AUSCERT that they are not vulnerable to these vulnerabilities:

Hewlett Packard
IBM Corporation
The OpenBSD project

If your vendor's name is not listed above, please contact your vendor directly. For more specific vendor information, see Appendix A.

3.3 Restrict crontab access

If the cron functionality is required by a small set of trusted users, sites may wish to restrict the execution of crontab to that group of users. For example, if the Unix group "trusted" exists and contains only those users allowed to use the cron functionality, the following commands will restrict its use:

```
# chgrp trusted /usr/bin/crontab
# chmod 4750 /usr/bin/crontab
# ls -l /usr/bin/crontab
-rwsr-x---  1 root    trusted  20480 Jun 10
1996 /usr/bin/crontab
```

Access to any account in the "trusted" group will allow vulnerable versions of the cron package to be exploited.

It should be noted that the use of cron allow/deny files (see crontab(1)) will not prevent the exploitation of the command line buffer overrun vulnerability.

Appendix A Vendor information

This appendix will be updated as we receive additional information. If your vendor is not listed below, or you require further vendor information, please contact the vendor directly.

FreeBSD, Inc.

FreeBSD versions 1.0, 1.1, 2.1.0, 2.1.5, 2.1.6, 2.1.6.1 and 2.2 -stable (prior to 16 Dec 1996) and 2.2 -current (prior to 16 Dec 1996) are all affected by the crontab vulnerabilities described in this advisory.

The FreeBSD Security Team have released an advisory and patch information for the crontab vulnerabilities. This advisory (FreeBSD-SA-96:20.stack-overflow) is available from:

ftp://freebsd.org/pub/CERT/advisories/FreeBSD-SA-96:20.stack-overflow.asc

Patches are available from:

ftp://freebsd.org/pub/CERT/patches/SA-96:20/

Hewlett Packard

The version of crontab shipped with all current versions of HP-UX 9.x and 10.x is not vulnerable to the buffer overflow problems described in this advisory.

IBM Corporation

The version of crontab shipped with AIX is not vulnerable to the buffer overflow conditions listed in this advisory.

IBM and AIX are registered trademarks of International Business Machines Corporation.

Linux (RedHat)

RedHat Linux version 4.0 is known to be vulnerable. Earlier versions may also be vulnerable.

The Net Project

All releases of NetBSD up to and including 1.2 appear to be vulnerable. These problems will be fixed in 1.3 and in the upcoming bug fix release for 1.2.

The OpenBSD Project

OpenBSD 2.0 is not susceptible to the vulnerabilities described in this advisory.

AUSCERT thanks Theo de Raadt of the OpenBSD project for his assistance in the preparation of this advisory. Thanks also to the vendors who provided specific product information.

[End AUSCERT Advisory]

CIAC wishes to acknowledge the contributions of AUSCERT for the information contained in this bulletin.

For additional information or assistance, please contact CIAC:
Voice: +1 510-422-8193 (8:00 - 18:00 PST, 16:00 - 2:00 GMT)
Emergency (DOE, DOE Contractors, and NIH ONLY):1-800-759-7243, 8550070 (primary),8550074 (secondary)
FAX: +1 510-423-8002
STU-III: +1 510-423-2604
E-mail: ciac@llnl.gov
World Wide Web: http://ciac.llnl.gov/
Anonymous FTP: ciac.llnl.gov (128.115.19.53)
Modem access: +1 (510) 423-4753 (28.8K baud), +1 (510) 423-3331 (28.8K baud)

This document was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor the University of California nor any of their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial products, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation or favoring by the United States Government or the University of California. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or the University of California, and shall not be used for advertising or product endorsement purposes.

UCRL-MI-119788

[Disclaimer]

Partitions and Directories

by Larry Ayers for the Linux Gazette (http://www.ssc.com/lg/)

After using linux for a while you tend to take for granted the supple flexibility inherent in the Linux manner of dealing with files, partitions, and mount-points. Recently I began to feel constrained by a relatively small /usr partition, so I thought I'd do some experimenting.

I happened to have an unused 100 mb. partition on my disk, so I created an ext-2 filesystem on it and mounted it on an empty directory, /new, created for this purpose. Then I ran this command: cp -a /usr/X11R6 /new. Using cp with the -a switch is really handy, as it copies all subdirectories, links, and files, and also saves permissions.

The next step was modifying the /etc/fstab file, inserting the following entry which causes /usr/X11R6 to be mounted on the new partition:

```
/dev/hda11 /usr/X11R6  ext2 defaults  1  2
```

Before rebooting I dropped back to a console and deleted the entire contents of the /usr/X11R6 directory. I was reasonably certain this would work, but I must confess I was surprised when (after rebooting) X started up without comment, as if nothing had changed.

Linux doesn't really care, after all, where files are located, as long as there is a congruence between the partition table and the contents of the /etc/fstab file. One benefit of this laxity is that repartitioning (with all of the attendant backing up, restoring, etc.) should seldom be necessary.

Contact Information

To contact the MUUG board for membership information or anything else, send e-mail to board@muug.mb.ca. We have a Web presence as well, at http://www.muug.mb.ca/, where you can find all kinds of information, including details of upcoming and past meetings and presentations and references related to them.

To contact the newsletter editor (and I know you want to shower him with dozens of well-written article submissions), e-mail editor@muug.mb.ca.