

Multiple Security Vulnerabilities in Fcron

iDEFENSE Security Advisory 11.15.04:

I. BACKGROUND

Fcron is a periodical command scheduler which aims at replacing Vixie Cron, and implements most of its functionalities. More information about Fcron is available from <http://fcron.free.fr/description.php>.

II. DESCRIPTION

Multiple vulnerabilities have been found in Fcron.

ISSUE 1 - File contents disclosure

Local exploitation of a design error vulnerability in the fcronsignup component of Fcron may allow users to view the contents of root owned files.

The vulnerability specifically exists within the set user id (setuid) root program fcronsignup. When the filename of a root owned file is passed as an argument to this program, it attempts to parse the file as a configuration file. Any lines in the file that are not parsable will be output as error messages. The following example demonstrates how an attacker can abuse this vulnerability to glean sensitive information from the /etc/shadow password file:

```
bash$ fcronsignup /etc/shadow
14:33:09 Unknown var name at line root:<password- hash>:12475:0:99999:7::: : line ignored
```

ISSUE 2 - Configuration Bypass Vulnerability

Local exploitation of a design error vulnerability in the fcronsignup component of Fcron may allow users to bypass access restrictions.

The problem specifically exists in the checking performed by the fcronsignup utility on the file passed as a configuration file. It checks if the file is root owned, and not writable by any other users.

When a setuid process is run by an ordinary user the /proc filesystem pseudofiles associated with it are owned by root and the contents of the "cmdline" and "environment" files are controllable by the user.

By pointing the fcronsignup configuration file to a /proc entry owned by root, such as /proc/self/cmdline or /proc/self/environ, it is possible for a user to supply their own configuration settings.

ISSUE 3 - File Removal and Empty File Creation Vulnerability

Local exploitation of a design error vulnerability in the fcronsignup component of Fcron may allow users to remove arbitrary files or create arbitrary empty files.

The vulnerability specifically exists in the fcronsignup utility which does signaling of the running fcrond daemon. Fcronsignup creates a file named in part from a value read from configuration file. This file is created using open() with O_RDWR|O_CREAT and 0644 parameters while running with full root privileges. After some time has passed the file is removed. The filename string is generated by the following code:

```
snprintf(sigfile, sizeof(sigfile), "%s/fcrontab.sig", fcrontabs);
```

By padding the front of the filename with a large number of slash symbols ("/") it is possible to create or remove a file in an arbitrary location. For example: to create the file /tmp/owned, the configuration option which sets the value for "fcrontabs" can be set to contain (sizeof(sigfile)- strlen("/tmp/owned")) "/" characters, followed by the string "/tmp/owned". The code will attempt to append the string "/fcrontab.sig" to this string, but the limitation imposed on it by the call to snprintf() will cause it to fail. When the filename is resolved, the extra "/"s in the filename are ignored, resulting in an absolute reference to the file /tmp/owned.

ISSUE 4 - Information Disclosure Vulnerability

Local exploitation of a design error vulnerability in the fcrontab component of Fcron may allow users to view the contents of fcron.allow and fcron.deny.

The problem specifically exists because Fcron leaks the file descriptors of the opened files /etc/fcron.allow and /etc/fcron.deny to the invoked editor. The default permissions on these files do not allow them to be read by unprivileged users:

```
-rw-r----- 1 root fcron 253 Jul 29 12:45 /etc/fcron.allow  
-rw-r----- 1 root fcron 255 Jul 29 12:45 /etc/fcron.deny
```

An attacker can exploit this vulnerability by setting the EDITOR environment variable to a program which outputs the contents of the open file descriptor; descriptor 3 to view the contents of fcron.allow and descriptor 4 to view the contents of fcron.deny.

III. ANALYSIS

Local users can bypass configuration settings, remove arbitrary files, create files with root permissions, read the contents of root owned files and send a SIGHUP to any process, potentially killing it. These actions may allow them to perform a denial of service or potentially elevate their privileges.

IV. DETECTION

iDEFENSE has confirmed that Fcron versions 2.0.1 and 2.9.4 are vulnerable. It is suspected that earlier versions are also affected.

V. WORKAROUND

Consider changing the permissions on the fcronsighup binary to only allow trusted users access. Make the binary only executable by users in the 'trusted' group by performing the following commands as root:

```
# chown root:trusted /usr/bin/fcronsighup  
# chmod 4110 /usr/bin/fcronsighup
```

Also consider performing the same operation on the fcrontab binary to prevent exploitation of Issue 4.

VI. VENDOR RESPONSE

The following releases are available to address these vulnerabilities:

2.0.2 : stable branch

<http://fcron.free.fr/archives/fcron-2.0.2.src.tar.gz> (France)

or

<ftp://ftp.seul.org/pub/fcron/fcron-2.0.2.src.tar.gz> (USA)

2.9.5.1 : dev branch

<http://fcron.free.fr/archives/fcron-2.9.5.1.src.tar.gz> (France)

or

<ftp://ftp.seul.org/pub/fcron/fcron-2.9.5.1.src.tar.gz> (USA)

VII. CVE INFORMATION

The Common Vulnerabilities and Exposures (CVE) project has assigned the following names to these issues:

ISSUE1 - File contents disclosure

CAN-2004-1030

ISSUE2 - Configuration Bypass Vulnerability

CAN-2004-1031

ISSUE3 - File Removal and Empty File Creation Vulnerability

CAN-2004-1032

ISSUE4 - Information Disclosure Vulnerability

CAN-2004-1033

These are candidates for inclusion in the CVE list

(<http://cve.mitre.org>), which standardizes names for security problems.