Published on *Jisc community* (https://community.jisc.ac.uk)

Advisory: FreeRADIUS 2.1.10,11,12 Security

September 2012 - 11/09/2012

This advisory applies to all FreeRADIUS based participants. Microsoft IAS, NPS, Cisco Secure ACS and other RADIUS server based participants are not affected.

Vulnerability

A vulnerability has been identified which affects setups using TLS-based EAP methods (including EAP-TLS, EAP-TTLS, and PEAP) i.e. pretty much all eduroam systems. The stack overflow vulnerability in FreeRADIUS versions 2.1.10 - 12 allows an attacker to remotely execute arbitrary code via specially crafted client certificates (before authentication).

An external attacker can use this vulnerability to over-write the stack frame of the RADIUS server, and cause it to crash. In addition, more sophisticated attacks may gain additional privileges on the system running the RADIUS server.

This attack does not require local network access to the RADIUS server. It can be done by an attacker through a Wi-Fi Access Point, so long as the Access Point is configured to use 802.1X authentication with the RADIUS server.

For information on the vulnerability announcement please consult:

http://freeradius.org/security.html [1]

http://www.pre-cert.de/advisories/PRE-SA-2012-06.txt [2]

Analysis

The pre-cert.de advisory states: FreeRADIUS defines a callback function cbtls_verify() for certificate verification. The function has a local buf array with a size of 64 bytes. It copies the validity timestamp "not after" of a client certificate to the buf array and if asn_time->length is greater than 64 bytes, but less than 254 bytes, buf overflows via the memcpy.

Our analysis is that whilst PEAP and TTLS don't *necessarily* use client certificates, with particular client configuration (and such deployments exist in the wild; they are just not very common in eduroam) after the server sends its certificate, a client can immediately answer with a client certificate during the tunnel establishment phase. (Username and passwords are still sent as usual within the tunnel).

The attack probably works by a client negotiating either TLS, PEAP, or TTLS, and unsolicitedly sending a specially crafted client certificate which exploits the vulnerability attack vector.

There is, as far as we know, no way to prevent the client from sending that client certificate. The server can opt to drop the connection after having received it (e.g. by configuring an empty list of CAs from which to accept client certificates), but will nevertheless go through the step of parsing the certificate before that.

Solution / Action Required

Upgrade to FreeRADIUS 2.2.0 immediately

If you are running 2.1.10, 11 or 12 you must upgrade immediately. Even if you are running an older version, you should upgrade to 2.2.0 at your earliest convenience. The older versions have known bugs and should not be used any more. Nb.All eduroam participants should ensure that eduroam servers and services are maintained according to the specified best practices for server build, configuration and security, with the purpose of maintaining a generally high level of security, and thereby trust in the eduroam Confederation.

Are there any implications in making the minor version jump? Only one single, very seldomly used parameter changes in an incompatible way. Quoting the release notes:

"100% configuration file compatible with 2.1.x. The only fix needed is to disallow 'hashsize=0' for rlm_passwd"

Stefan has already upgraded RESTENA's fleet of FreeRADIUS servers and has reported that there were no unwanted side-effects.

Where to get the latest Version of FreeRADIUS

You can download the latest 2.2.0 from freeradius.org and build it from here:

http://freeradius.org/download.html [3]

Also, binary packagesfor a number of platforms are available from third parties. If you want to remain with a repository version, you will have to wait until RedHat / CentOS update the yum repository.

Upgrade Hint

'FR 2.2.0 includes this feature: DHCP capabilitiies are now compiled in by default. But it runs as a DHCP server ONLY when manually enabled.'

We had an early report that after having made the upgrade (via make install) there was a need to rename modules/dhcp_sqlippool otherwise the server complained about an error.

```
"...including configuration file /usr/local/etc/raddb/modules/mac2ip
```

```
including configuration file
/usr/local/etc/raddb/modules/dhcp_sqlippool

including configuration file /usr/local/etc/raddb/sql/mysql/ippool-
dhcp.conf

Unable to open file "/usr/local/etc/raddb/sql/mysql/ippool-
dhcp.conf": No such file or directory

Errors reading or parsing /usr/local/etc/raddb/radiusd.conf"
```

The participant was not using FR as a DHCP server, so they just prepended % to the name and everything was OK. Alternatively you could remove the modules/dhcp_sqlippool file.

Evidently the DHCP engine of FR 2.2.0 is now present/active by default; the new module definition is installed and for some reason also activated.

Usually, when you do a "make install", FreeRADIUS 2.x will add all new modules into your modules/ directory. That is not usually a problem, because the module will only be loaded if you reference it in one of the virtual server in sites-enabled/ . So, the current behaviour is surprising and if it is commonly experienced it might be a question to ask at the FR mailing list since it may be just a bug.

You can avoid any similar problems/surprises in the future by adopting the following procedure:

If you prevent FreeRADIUS' "make install" from affecting your existing config, unexpected surprises can be avoided. The trick is to rename the new source tarball's raddb/ subdirectory to raddb-noinst/ or similar right before typing "make install". The server will then ignore the missing raddb/ directory and not do any updates to the config.

The drawback of this is that you miss new features that would go into the config. The upside is that you miss new features that can adversely affect the server.

Acknowledgements:

Thanks to Stefan Winter of Fondation RESTENA for contributions to analysis and upgrade hints sections.

Source URL: https://community.jisc.ac.uk/library/janet-services-documentation/advisory-freeradius-21101112-security

Links
[1] http://freeradius.org/security.html
[2] http://www.pre-cert.de/advisories/PRE-SA-2012-06.txt
[3] http://freeradius.org/download.html