Advisory: OpenSSL TLS Heartbleed Vulnerability

Advisory issued by eduroam.OT 08/04/2014

It has come to our attention that there are vulnerabilities in the relatively new 1.0.1-series of OpenSSL (as detailed by http://heartbleed.com/ [1]) affecting TLS enabled services via a heartbeat extension.

While there are no indications that this affects TLS-based EAP-mechanisms or RADIUS/TLS (aka RadSec) at this time, the operational team has made the decision to upgrade OpenSSL to versions implementing a fix for CVE-2014-0160

We advise roaming operators to bring this CVE-2014-0160 to the attention of eduroam administrators, so they can investigate their systems and upgrade when systems are running affected versions.

Progress and updates on this note will be published on the TERENA wiki, at https://confluence.terena.org/display/H2eduroam/heartbleed-note [2]

WARNING: Expect that from mid-April, the threat will become more severe, and be aware that remediation is extremely difficult. Because the eduroam authentication takes place before getting access to a network, it's not possible to consult a certificate revocation list (CRL) or query the certificate status online (with OCSP). As exploits on HTTPS already exist and can probably be ported to TLS over EAP, we have only limited time to react to this threat.

14/4/14: eduroam.OT has had first-to-see access to the exploit code and consequently has been able to run the vulnerability tests for the eduroam community systematically since late last week. This means that we have a time advantage to fix our collective infrastructure.

However, the code will not remain secret; the knowledge that such code exists is already out there, so even if the code itself doesn't leak, someone with skill and time can just replicate code achieving the same functionality on their own.

Together with others from the GeGC, eduroam.OT has created a rough timeline towards informing CERTs and, at some point, allowing the code author to release his code. From that moment on, you either have fixed your server, or are in for a bit of trouble.

The timeline is roughly as follows:

- near the end of this week (e.g. 17th April), inform the TI Accredited CERT community that easily exploitable attack vectors against TLS over EAP exist

- near the end of next week (e.g. 24/4/14), give the code author clearance to publish his code (note that we can't order him to do anything, if he wants to do it earlier, he can; he is cooperative though).

Statement from FreeRADIUS 08/04/2013

FreeRADIUS has released a statement on the OpenSSL security issue: http://freeradius.org/security.html [3]

In short, versions 2 and 3 are vulnerable but not to the scale of e.g. other SSL/TLS implementations and it is recommended that FR sites immediately upgrade OpenSSL. (This is the same stance as adopted by other vendors).

Statement from OSC regarding RADIATOR RADIUS platform 09/04/2014

We have now done further testing and have verified that the OpenSSL vulnerability described in CVE-2014-0160 [1] affects Radiator too.

Please see the CVE for more information about the vulnerability. The URL is below.

We strongly recommend that the administrators update the OpenSSL installation Radiator uses to a version that is not vulnerable. To help with the OpenSSL update, we have identified a number of possibilities. Note: this list is not meant to be exhaustive.

With Linux and other Unix type of systems, the required OpenSSL update typically means applying the patches from the operating system provider. These patches are already available for many operating systems.

Windows ActivePerl and Strawberry Perl users should see what updates are available from these Perl providers.

An additional possibility on any system for updating OpenSSL to a non vulnerable version is to locally compile a new version of OpenSSL. This may also require compiling Perl Net-SSLeay that links to the OpenSSL libraries.

As an interim option, Windows ActivePerl and Strawberry Perl users may also consider the precompiled Net-SSLeay PPM modules OSC has previously made available. These modules come with OpenSSL 0.9.8 which is not vulnerable according to CVE-2014-0160. Net-SSLeay is often used by Radiator when SSL/TLS is needed, so this module will help to mitigate the vulnerability while all the vulnerable OpenSSL versions are being updated.

We have tested the precompiled Net-SSLeay PPM modules with 32 and 64 bit ActivePerl and Strawberry Perl versions 5.16.3 and 5.14.4 and found them non-vulnerable. We have not tested with other Perl versions, but we believe the precompiled Net-SSLeay PPM modules for the other Perl versions are not vulnerable either.

The precompiled Net-SSLeay PPM modules are available from OSC's web site: https://www.open.com.au/radiator/free-downloads/ [4]

The future Radiator versions will try to detect OpenSSL with this vulnerability with an option to turn off the detection if required.

References:

[1] http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0160 [5]

Statement from Cisco 14/4/2014

"Cisco Secure Access Control Server (ACS)" has been analyzed and is not affected.

Full statement and list of affected/unaffected products:

http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20140409-heartbleed [6]

eduroam(UK) advice

In addition to above, you should read the Janet CSIRT blog entry:

https://community.ja.net/blogs/csirt/article/heartbleed-openssl-vulnerability-cve-2014-0160 [7]

Please also note that some distributions - eg CentOS 6 or RedHat 6 are actually releasing a version of e.g 1.0.1e that has the backport fix and heartbeat still enabled - you will need to use a suitable security tool to validate/verify that your system is patched.

Finally, after patching OpenSSL you will need to either restart all services using OpenSSL (as they will have loaded the old libraries) - eg restart FreeRADIUS or Apache HTTPD - or reboot/reload the server.

The potential exploitation of RADIUS has several mitigating factors: it is more difficult to exploit than other implementations as it is considerably harder to write TLS over EAP over RADIUS exploit code than normal TLS over TCP. The focus of attacks to the present has been the large number of unpatched web and mail servers. RADIUS expolitation is also detectable: administrators can detect 'heartbleed' attacks by looking in their logs for a message containing the text Invalid ACK received: 24. If such a message is seen, it means that the attack has been attempted.

Nevertheless, eduroam.OT is taking a proactive safety-first stance and has been able to produce a special eapol_test tool to test vulnerability of realms in the eduroam confederation. The tool sends the bogus heartbeat extension request but only calls for 10 Byte of your server memory which is not large enough for your secret key to be compromised. The test will use User-Name = heartbleed.test@<the realm> Operator-Name = 1eduroam.ot.heartbleed.test. The admins of vulnerable realms will be contacted directly. Initially only servers in the CAT database were being tested, however the test is now available for all RADIUS servers registered in the eduroam database.

Due to the terms of the Computer Misuse Act and Janet's AUP, eduroam(UK) is not permitted to probe your RADIUS servers to test for this vulnerability without your consent. To enable you to give us consent to test for this and any future vulnerabilities, a tick box has been introduced on the Support server. In relation to this specific OpenSSL vulnerability, we will use this to advise eduroam.OT that you have given permission for the test to be carried out and we will advise you if a vulnerability is found. Nb. The test only reports on the RADIUS server at your realm that responds and may return false positives. It cannot be taken as a guarantee that your RADIUS servers are secure.

Source URL: https://community-stg.jisc.ac.uk/library/janet-services-documentation/advisory-openssl-tls-heartbleed-vulnerability

Links
[1] http://heartbleed.com/
[2] https://confluence.terena.org/display/H2eduroam/heartbleed-note
[3] http://freeradius.org/security.html
[4] https://www.open.com.au/radiator/free-downloads/
[5] http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0160
[6] http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20140409-heartbleed
[7] https://community.ja.net/blogs/csirt/article/heartbleed-openssl-vulnerability-cve-2014-0160