Tartu Ülikool
Loodus- ja täppiteaduste valdkond
Arvutiteaduse instituut

Andmeturve
Referaat
CVE-2016-4979

Koostaja: Richardas Keršis
Juhendaja: Meelis Roos

Tartu 2017
Introduction

The Apache HTTP Server is the world’s most used web server. Web servers store, process and deliver web pages to clients via HTTP. Apache HTTP Server introduced an experimental feature mod_http2 with the release of version 2.4.17 which provides HTTP/2 support. To use the feature, HTTP/2 (which uses two schemes (HTTP/2 over TLS) and h2c (HTTP/2 over TCP)) must be enabled via Protocols configuration. This feature (module) had a vulnerability described below.

Vulnerability description

For the enabled HTTP/2 configuration SSL client certificate validation was not enforced (server failed to take the (failed/absent) X509 client certificate validation into account). As a result, resource (client) was thought to be secure and providing valid client certificate when the experimental mod_http2 module was used to acces a resource. This vulnerability affected all Apache HTTP Server versions from 2.4.18 to 2.4.20. This issue was fixed in version 2.4.23.

Exploitation

This vulnerability let remote and third party users to bypass client certificate authentication by leveraging the ability to send multiple requests over a single connection, which led to aborting a renegotiation, thus, getting access to protected resources over HTTP/2. So, if the remote user (attacker) was to send multiple requests over a single connection, the authentication request would eventually fail to be repeated and client certificate would not be taken into account, letting attacker through client certificate validation.
Solution

As a temporary solution, HTTP/2 could be disabled in the Protocols directive. But the problem was resolved by Stefan Eissing. The solution to the problem was to reset client-verify state of ssl when aborting renegotiations so that the authorization request is repeated. Hence, next line of code was added:

```c
SSL_set_verify(ssl, verify_old, ssl_callback_SSLVerify);
```

Clients should use/update to the Apache HTTP Server versions above 2.4.23, where this issue is fixed.

References

- [https://github.com/apache/httpd/commit/2d0e4eff04ea963128a41faaef21f987272e05a2](https://github.com/apache/httpd/commit/2d0e4eff04ea963128a41faaef21f987272e05a2)
- [https://httpd.apache.org/docs/2.4/mod/mod_http2.html](https://httpd.apache.org/docs/2.4/mod/mod_http2.html)