CERT-EU Security Advisory 2017-002

Ticketbleed Vulnerability Affecting F5 BIG-IP

February 9, 2017 — v1.0

History:

- *09/01/2017 — v1.0 – Initial publication*

Summary

A vulnerability in F5 BIG-IP devices (CVE-2016-9244 [1]) could allow an unauthenticated, remote attacker to obtain sensitive information from memory if the non-default *Session Tickets* option is enabled for a Client SSL profile.

The vulnerability allows the attacker to retrieve up to 31 bytes of uninitialized memory at a time. This memory can potentially contain key material or sensitive data from other connections like Secure Sockets Layer (SSL) session IDs.

The vulnerability is called **Ticketbleed** [2], and F5 Product Development has assigned ID 596340 (BIG-IP) to this vulnerability [3].

Products Affected

This vulnerability affects BIG-IP virtual server component on several F5 BIG-IP products.

The following versions of the BIG IP products are affected by the vulnerability described in this document:

- versions `12.0.0` to `12.1.2` and `11.4.0` to `11.6.1` of the BIG-IP LTM, BIG IP AAM, BIG-IP AFM, BIG-IP Analytics, BIG-IP APM, BIG-IP ASM, BIG-IP Link Controller, and BIG-IP PEM
- versions `11.4.0` to `11.6.1` of the BIG-IP GTM
- versions `11.4.0` to `11.4.1` of the BIG-IP PSM

Recommendations

Versions `11.4.0` to `11.6.1` of the affected products (except BIG-IP PSM) can be upgraded to patched version `11.6.1 HF2`. For affected products using versions `12.0.0` to `12.1.2`, no patched version currently exists.

A workaround is to disable the *Session Ticket* option on the affected Client SSL profile. To do so, perform the following procedure:

- Log in to the *Configuration* utility.
- Navigate to **Local Traffic** > **Profiles** > **SSL** > **Client**.
- For the **Configuration** option, select **Advanced**.
- Clear the **Session Ticket** check box.
- Click **Update**.

References

[1] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-9244

[2] https://filippo.io/Ticketbleed/

[3] https://support.f5.com/csp/article/K05121675