Security Advisory 2020-042

XSS Vulnerability in F5 BIG-IP

August 28, 2020 — v1.0

TLP:WHITE

History:

- *28/08/2020 — v1.0 – Initial publication*

Summary

An HTML-injection vulnerability (CVE-2020-5915) has been discovered affecting multiple F5 BIG-IP Products [1]. Insufficient sanitisation of user input in *Traffic Management User Interface (TMUI)* or *Configuration Utility* component can potentially allow an attacker to execute arbitrary commands [2].

Technical Details

An attacker with *Resource Administrator* or *Administrator* privileges may exploit the vulnerability to inject HTML or JavaScript code into a vulnerable section of the application. For a logged in user – while viewing the affected section – the injected code is rendered. Theoretically, the attacker can steal cookie-based authentication credentials and control how the site is rendered to the user. More client side attack technics and impact may also be observed.

Currently, there is not known proof of concept or exploits.

Products Affected

According to the vendor the following products of BIG-IP (LTM, AAM, AFM, Analytics, APM, ASM, DNS, Edge Gateway, FPS, GTM, Link Controller, PEM, WebAccelerator) are affected:

- 15.0.0 - 15.1.0,
- 14.0.0 - 14.1.2,
- 13.1.0 - 13.1.3,
- 12.1.0 - 12.1.5,
- 11.5.2 - 11.6.4.

Recommendations

The vendor and CERT-EU recommend to upgrade a vulnerable software to a respective version as shown below [2]:

- 15.1.0.5,
- 15.0.1.4,
- 14.1.2.4,
- 13.1.3.4,
- 12.1.5.2,
- 11.6.5.2.

Workarounds

Secure access to the BIG-IP system to ensure that the TMUI is only accessible by trusted users.

As a best practice, run all software as a non-privileged user with minimal access rights. This may limit the immediate consequences of client-side vulnerabilities.

References

[1] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-5915

[2] https://support.f5.com/csp/article/K57214921