Security Advisory 2021-044

Critical Vulnerabilities Affecting F5 Devices

August 27, 2021 — v1.0

TLP:WHITE

History:

- *27/08/2021 — v1.0 – Initial publication*

Summary

On the 24th or August 2021, F5 released several security advisories affecting multiple versions of BIG-IP and BIG-IQ devices [1]. Among them, there is one **critical** vulnerability – CVE-2021-23031 – that is affecting BIG-IP Advanced Web Application Firewall and BIG-IP Application Security Manager. It allows an authenticated user to perform a privilege escalation [2].

Technical Details

From the security advisory [1]:

CVE-2021-23031

BIG-IP Advanced WAF and BIG-IP ASM vulnerability (K41351250) - CVSS score: 8.8 (high) and 9.9 (Critical) for appliance mode only

When exploited, an authenticated attacker with access to the Configuration utility can execute arbitrary system commands, create or delete files, and/or disable services. This vulnerability may result in complete system compromise.

CVE-2021-23025

BIG-IP TMUI vulnerability (K55543151) - CVSS score: 7.2 (High)

An authenticated remote command execution vulnerability exists in the BIG-IP Configuration utility.

CVE-2021-23026

BIG-IP TMUI vulnerability (K53854428) - CVSS score: 7.5 (High)

BIG-IP and BIG-IQ are vulnerable to cross-site request forgery (CSRF) attacks through iControl SOAP.

CVE-2021-23027

TMUI XSS vulnerability (K24301698) - CVSS score: 7.5 (High)

A DOM based cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Configuration utility that allows an attacker to execute JavaScript in the context of the currently logged-in user.

CVE-2021-23028

BIG-IP Advanced WAF and ASM vulnerability (K00602225) - CVSS score: 7.5 (High)

When JSON content profiles are configured for URLs as part of an F5 Advanced Web Application Firewall (WAF)/BIG-IP ASM security policy and applied to a virtual server, undisclosed requests may cause the BIG-IP ASM bd process to terminate.

CVE-2021-23029

BIG-IP Advanced WAF and ASM TMUI vulnerability (K52420610) - CVSS score: 7.5 (High)

Insufficient permission checks may allow authenticated users with guest privileges to perform Server-Side Request Forgery (SSRF) attacks through F5 Advanced Web Application Firewall (WAF) and the BIG-IP ASM Configuration utility.

CVE-2021-23030

BIG-IP Advanced WAF and ASM Websocket vulnerability (K42051445) - CVSS score: 7.5 (High)

When a WebSocket profile is configured on a virtual server, undisclosed requests can cause bd to terminate.

CVE-2021-23032

BIG-IP DNS vulnerability (K45407662) - CVSS score: 7.5 (High)

When a BIG-IP DNS system is configured with non-default Wide IP and pool settings, undisclosed DNS responses can cause the Traffic Management Microkernel (TMM) to terminate.

CVE-2021-23033

BIG-IP Advanced WAF and ASM Websocket vulnerability (K05314769) - CVSS score: 7.5 (High)

When a WebSocket profile is configured on a virtual server, undisclosed requests can cause bd to terminate.

CVE-2021-23034

BIG-IP TMM vulnerability (K30523121) - CVSS score: 7.5 (High)

When a DNS profile using a DNS cache resolver is configured on a virtual server, undisclosed requests can cause the Traffic Management Microkernel (TMM) process to terminate.

CVE-2021-23035

TMM vulnerability (K70415522) - CVSS score: 7.5 (High)

When an HTTP profile is configured on a virtual server, after a specific sequence of packets, chunked responses can cause the Traffic Management Microkernel (TMM) to terminate.

CVE-2021-23036

TMM vulnerability (K05043394) - CVSS score: 7.5 (High)

When a BIG-IP ASM and DataSafe profile are configured on a virtual server, undisclosed requests can cause the Traffic Management Microkernel (TMM) to terminate.

CVE-2021-23037

TMUI XSS vulnerability (K21435974) - CVSS score: 7.5 (High)

A reflected cross-site scripting (XSS) vulnerability exists in an undisclosed page of the BIG-IP Configuration utility that allows an attacker to execute JavaScript in the context of the currently logged-in user.

Affected Products

- CVE-2021-23031 affects BIG-IP (Advanced WAF and ASM) before 16.1.0, 16.0.1.2, 15.1.3, 14.1.4.1, 13.1.4, 12.1.6, 11.6.5.3

For the other CVEs please consult the table available on F5 advisory [1].

Recommendations

Apply the patches as soon as possible.

References

[1] https://support.f5.com/csp/article/K50974556

[2] https://support.f5.com/csp/article/K41351250