CERT-EU
FOR THE EU INSTITUTIONS, BODIES AND AGENCIES

Security Advisory 2021-015

Critical Vulnerabilities Affecting F5 Devices

March 18, 2021 — v1.1

TLP:WHITE

History:

- *11/03/2021 — v1.0 – Initial publication*
- *18/03/2021 — v1.1 – Update to include proof-of-concept*

Summary

On the 10th or March 2021, F5 released several security advisories, including four identified as **critical** [1].

One of the vulnerabilities allows an unauthenticated attacker with network access to the iControl REST interface, through the BIG-IP management interface and self IP addresses, to execute arbitrary system commands, create or delete files, and disable services [2].

Another of the vulnerabilities may allow either a bypass of URL-based access control or remote code execution (RCE) if a request is incorrectly handled by Traffic Management Microkernel (TMM) URI normalisation [3].

A Proof-Of-Concept for the iControl vulnerability (CVE-2021-22986) has been released by a security researcher [4]. The attacker needs access to the management interface to use the exploit.

Technical Details

Information extracted from F5 advisories [1]:

CVE-2021-22986: iControl REST unauthenticated remote command execution vulnerability (K03009991)

The iControl REST interface has an unauthenticated remote command execution vulnerability.

CVSS score: 9.8 (Critical)

CVE-2021-22987: Appliance Mode TMUI authenticated remote command execution vulnerability (K18132488)

When running in Appliance mode, the Traffic Management User Interface (TMUI), also referred to as the Configuration utility, has an authenticated remote command execution vulnerability in undisclosed pages.

CVSS score: 9.9 (Critical)

CVE-2021-22988: TMUI authenticated remote command execution vulnerability (K70031188)

TMUI, also referred to as the Configuration utility, has an authenticated remote command execution vulnerability in undisclosed pages.

CVSS score: 8.8 (High)

CVE-2021-22989: Appliance mode Advanced WAF/ASM TMUI authenticated remote command execution vulnerability (K56142644)

When running in Appliance mode with Advanced WAF or BIG-IP ASM provisioned, the TMUI, also referred to as the Configuration utility, has an authenticated remote command execution vulnerability in undisclosed pages.

CVSS score: 8.0 (High)

CVE-2021-22990: Advanced WAF/ASM TMUI authenticated remote command execution vulnerability (K45056101)

On systems with Advanced WAF or BIG-IP ASM provisioned, the TMUI, also referred to as the Configuration utility, has an authenticated remote command execution vulnerability in undisclosed pages.

CVSS score: 6.6 (Medium)

CVE-2021-22991: TMM buffer-overflow vulnerability (K56715231)

Undisclosed requests to a virtual server may be incorrectly handled by the Traffic Management Microkernel (TMM) URI normalization, which may trigger a buffer overflow, resulting in a DoS attack. In certain situations, it may theoretically allow bypass of URL based access control or remote code execution (RCE).

CVSS score: 9.0 (Critical)

CVE-2021-22992: Advanced WAF/ASM buffer-overflow vulnerability (K52510511)

A malicious HTTP response to an Advanced WAF/BIG-IP ASM virtual server with Login Page configured in its policy may trigger a buffer overflow, resulting in a DoS attack. In certain situations, it may allow remote code execution (RCE), leading to complete system compromise.

CVSS score: 9.0 (Critical)

Affected Products

- BIG-IP before 16.0.1.1, 15.1.2.1, 14.1.4, 13.1.3.6, 12.1.5.3, and 11.6.5.3
- CVE-2021-22986 also affects BIG-IQ before 8.0.0, 7.1.0.3, and 7.0.0.2

Depending on the deployment mode, some vulnerabilities may not apply. To get more detail, 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/K02566623

[2] https://support.f5.com/csp/article/K03009991

[3] https://support.f5.com/csp/article/K56715231

[4] https://attackerkb.com/topics/J6pWeg5saG/k03009991-icontrol-rest-unauthenticated-remote-command-execution-vulnerability-cve-2021-22986