CERT-EU

Security Advisory 2025-037

Multiple Vulnerabilities in F5 Products

2025-10-15 — v1.0

TLP:CLEAR

History:

- *15/10/2025 — v1.0 – Initial publication*

Summary

On October 15, 2025, F5 disclosed that a sophisticated nation-state actor breached its systems and maintained long-term persistent access into F5's infrastructure [1]. This included access to BIG-IP product development source code and to information related to security vulnerabilities that had not yet been disclosed nor patched. F5 released patches on the same day to address the vulnerabilities [2].

There is currently no known exploitation of these vulnerabilities. CERT-EU strongly recommends to patch affected F5 products as soon as possible.

Technical Details

The vulnerability **CVE-2025-53868**, with a CVSS score of 8.5, is affecting all modules of BIG-IP and could allow a highly privileged authenticated attacker with access to Secure Copy (SCP) protocol and SFTP to bypass Appliance mode restrictions using undisclosed commands. [3]

The vulnerability **CVE-2025-61955** and **CVE-2025-57780**, with a CVSS score of 8.5, are affecting F5OS and could allow an authenticated attacker with local access to escalate their privileges. A successful exploit may allow the attacker to cross a security boundary. [4,5]

The exhaustive list of vulnerabilities can be found in the F5 Quarterly Security Notification.

Affected Products

BIG-IP, F5OS, BIG-IP Next for Kubernetes, BIG-IQ, and APM are affected by the vulnerabilities [1].

Refer to F5's advisory for the list of all affected products. [2]

Recommendations

CERT-EU recommends to apply updates on affected F5 products as soon as possible.

References

[1] https://my.f5.com/manage/s/article/K000154696

[2] https://my.f5.com/manage/s/article/K000156572#high

[3] https://my.f5.com/manage/s/article/K000151902

[4] https://my.f5.com/manage/s/article/K000156767

[5] https://my.f5.com/manage/s/article/K000156771