F5 BIG-IP Source Code Leaked in State-Linked Cyberattack (BRICKSTORM Malware) – Qualys ThreatPROTECT

By Author: Diksha Ojha Senior Technical Writer View all posts by Diksha Ojha

Published: 2025-10-17 · Archived: 2026-04-06 00:04:28 UTC

F5 Networks warned its users about a widespread cyberattack that compromised its systems and led to the theft of BIG-IP source code and details of unpatched security vulnerabilities.

In the article, F5 describes becoming aware of the breach in August 2025. A highly sophisticated nation-state threat actor maintained long-term, persistent access to, and downloaded files from, specific F5 systems, including the BIG-IP product development environment and engineering knowledge management platforms.

F5 mentioned in the article that “we are taking proactive measures to protect our customers and strengthen the security posture of our enterprise and product environments. We have engaged CrowdStrike, Mandiant, and other leading cybersecurity experts to support this work, and we are actively engaged with law enforcement and our government partners.”

In its October 2025 Quarterly Security Notification, F5 released updates for BIG-IP, F5OS, and BIG-IP Next for Kubernetes, BIG-IQ, and APM clients.

Discovery

The data breach started with threat actors extracting files from the BIG-IP product development environment and engineering knowledge management platforms. Those files contained some of the BIG-IP source code and information about undisclosed vulnerabilities existing in BIG-IP.

The vendor has no evidence of access to, or extraction of, data from their CRM, financial, support case management, or iHealth systems. However, some of the extracted files from the knowledge management platform contained configuration or implementation information for a small percentage of customers.

CISA Emergency Directive (ED 26-01)

In immediate response to the breach, the Cybersecurity and Infrastructure Security Agency (CISA) issued an Emergency Directive (ED 26-01). The directive instructs all Federal Civilian Executive Branch agencies to inventory F5 BIG-IP devices, ensure management interfaces are inaccessible from the public internet, apply all newly released updates by October 22, 2025, and report full compliance by October 29, 2025.

CISA warned that the stolen information gives attackers an unfair advantage in performing vulnerability research and potentially crafting zero-day exploits against unpatched systems.

Google, Mandiant, and CrowdStrike investigations revealed links between the F5 data breach and a Chinese cyber espionage group called UNC5221. Bloomberg later reported that the attackers had infiltrated F5’s network for

over 12 months, using custom malware identified as BRICKSTORM. This spyware is believed to have been deployed against organizations in technology, legal services, SaaS, and BPO sectors in similar campaigns across the U.S.

The Mandiant team has released a BRICKSTORM Indicator of Compromise Scanner to detect potential BRICKSTORM backdoor compromises on Linux and BSD-based appliances and systems. The script is designed to replicate the logic of a specific YARA rule on systems where YARA is not available or practical to run.

Affected and Fixed Versions

CVE	Affected Versions	Fixed Versions
CVE-2025-53868	BIG-IP all modules: 17.5.0, 17.1.0 – 17.1.2, 16.1.0 – 16.1.6, 15.1.0 – 15.1.10	17.5.1, 17.1.3, 16.1.6.1, 15.1.10.8
CVE-2025-61955	F5OS-A: 1.8.03, 1.5.1 – 1.5.3; F5OS-C: 1.8.0 – 1.8.1, 1.6.0 – 1.6.23	F5OS-A: 1.8.3, 1.5.4; F5OS-C: 1.8.2, 1.6.4
CVE-2025-57780	F5OS-A: 1.8.03, 1.5.1 – 1.5.3; F5OS-C: 1.8.0 – 1.8.1, 1.6.0 – 1.6.23	F5OS-A: 1.8.3, 1.5.4; F5OS-C: 1.8.2, 1.6.4
CVE-2025-60016	BIG-IP all modules: 17.1.0 – 17.1.1; BIG-IP Next SPK: 1.7.0 – 1.9.2; BIG-IP Next CNF: 1.1.0 – 1.3.3	BIG-IP all modules: 17.1.2; BIG-IP Next CNF: 2.0.0, 1.4.0
CVE-2025-48008	BIG-IP all modules: 17.1.0 – 17.1.2, 16.1.0 – 16.1.5, 15.1.0 – 15.1.10	17.1.2.2, 16.1.6, 15.1.10.8
CVE-2025-59781	BIG-IP all modules: 17.1.0 – 17.1.2, 16.1.0 – 16.1.5, 15.1.0 – 15.1.10	17.1.2.2, 16.1.6, 15.1.10.8
CVE-2025-41430	BIG-IP SSL Orchestrator: 17.5.0, 17.1.0 – 17.1.2, 16.1.0 – 16.1.3, 15.1.0 – 15.1.9	17.5.1, 17.1.3, 16.1.4
CVE-2025-55669	BIG-IP ASM: 17.1.0 – 17.1.2, 16.1.0 – 16.1.5	17.1.2.2, 16.1.6
CVE-2025-	BIG-IP all modules: 17.5.0, 17.1.0 – 17.1.2, 16.1.0 – 16.1.6	17.5.1, 17.1.3, 16.1.6.1

61951		
CVE-2025-55036	BIG-IP SSL Orchestrator: 17.1.0 – 17.1.2, 16.1.0 – 16.1.5, 15.1.0 – 15.1.10	17.1.3, 16.1.6, 15.1.10.8
CVE-2025-54479	BIG-IP PEM: 17.5.0, 17.1.0 – 17.1.2, 16.1.0 – 16.1.6, 15.1.0 – 15.1.10; BIG-IP Next CNF: 2.0.0 – 2.1.0, 1.1.0 – 1.4.0	17.5.1, 17.1.3, 16.1.6.1, 15.1.10.8; BIG-IP Next CNF: 2.1.0 (EHF-14, EHF-24, EHF-34)
CVE-2025-46706	BIG-IP all modules: 17.1.0 – 17.1.2, 16.1.0 – 16.1.5	17.1.2.2, 16.1.6
CVE-2025-59478	BIG-IP AFM: 17.5.0, 17.1.0 – 17.1.2, 15.1.0 – 15.1.10	17.5.1, 17.1.3, 15.1.10.8
CVE-2025-61938	BIG-IP Advanced WAFASM: 17.5.0, 17.1.0 – 17.1.2	17.5.1, 17.1.3
CVE-2025-54858	BIG-IP Advanced WAFASM: 17.5.0 – 17.5.1, 17.1.0 – 17.1.2, 16.1.0 – 16.1.6, 15.1.0 – 15.1.10	17.5.1.3, 17.1.3, 16.1.6.1, 15.1.10.8
CVE-2025-58120	BIG-IP Next SPK: 2.0.0, 1.7.0 – 1.7.14; BIG-IP Next CNF: 2.0.0, 1.1.0 – 1.4.1	2.0.1, 1.7.14 (EHF-24); 2.0.1
CVE-2025-53856	BIG-IP all modules: 17.5.0 – 17.5.1, 17.1.0 – 17.1.2, 16.1.0 – 16.1.6, 15.1.0 – 15.1.10	17.5.1.3, 17.1.3, 16.1.6.1, 15.1.10.8
CVE-2025-61974	BIG-IP all modules: 17.5.0 – 17.5.1, 17.1.0 – 17.1.2, 16.1.0 – 16.1.6, 15.1.0 – 15.1.10	17.5.1.3, 17.1.3, 16.1.6.1, 15.1.10.8; BIG-IP Next SPK: 2.0.0 – 2.0.2; BIG-IP Next CNF: 2.0.0 – 2.1.0
CVE-2025-58071	BIG-IP all modules: 17.5.0, 17.1.0 – 17.1.2, 16.1.0 – 16.1.6, 15.1.0 – 15.1.10; BIG-IP Next CNF: 2.0.0 – 2.1.0, 1.1.0 – 1.4.1	17.5.1, 17.1.3, 16.1.6.1, 15.1.10.8; BIG-IP Next CNF: 2.1.0 (EHF-14, EHF-24, EHF-34)
CVE-2025-53521	BIG-IP APM: 17.5.0 – 17.5.1, 17.1.0 – 17.1.2, 16.1.0 – 16.1.6, 15.1.0 – 15.1.10	17.5.1.3, 17.1.3, 16.1.6.1, 15.1.10.8

CVE-2025-61960	BIG-IP APM: 17.5.0 – 17.5.1, 17.1.0 – 17.1.2, 16.1.0 – 16.1.6	17.5.1.3, 17.1.3, 16.1.6.1
CVE-2025-54854	BIG-IP APM: 17.5.0 – 17.5.1, 17.1.0 – 17.1.2, 16.1.0 – 16.1.6, 15.1.0 – 15.1.10	17.5.1.3, 17.1.3, 16.1.6.1, 15.1.10.8
CVE-2025-53474	BIG-IP APM: 17.5.0 – 17.5.1, 17.1.0 – 17.1.2, 16.1.0 – 16.1.6, 15.1.0 – 15.1.10	17.5.1.3, 17.1.3, 16.1.6.1, 15.1.10.8
CVE-2025-61990	BIG-IP all modules: 17.5.0 – 17.5.1, 17.1.0 – 17.1.2, 16.1.0 – 16.1.6, 15.1.0 – 15.1.10	17.5.1.3, 17.1.3, 16.1.6.1, 15.1.10.8; BIG-IP Next SPK: 2.0.0 – 2.0.2; BIG-IP Next CNF: 2.0.0 – 2.1.0
CVE-2025-58096	BIG-IP all modules: 17.5.0 – 17.5.1, 17.1.0 – 17.1.2, 16.1.0 – 16.1.6, 15.1.0 – 15.1.10	17.5.1.3, 17.1.3, 16.1.6.1, 15.1.10.8
CVE-2025-61935	BIG-IP Advanced WAFASM: 17.5.0, 17.1.0 – 17.1.2, 15.1.0 – 15.1.10	17.5.1, 17.1.3

For more information, please refer to the October 2025 Quarterly Security Notification.

Qualys Detection

Note: All the QIDs mentioned below are only scanner-supported (Authenticated remote scanning).

CVE	**QID**
CVE-2025-58474	385574
CVE-2025-55036	385571
CVE-2025-61938	385573
CVE-2025-41430	385572
CVE-2025-53474	385544
CVE-2025-59268	385543
CVE-2025-59269	385560
CVE-2025-47148	385562

CVE-2025-59478	385556
CVE-2025-60016	385567
CVE-2025-58153	385548
CVE-2025-48008	385561
CVE-2025-55669	385540
CVE-2025-46706	385547
CVE-2025-59781	385566
CVE-2025-58424	385555
CVE-2025-54479	385541
CVE-2025-53856	385568
CVE-2025-61951	385559
CVE-2025-61935	385550
CVE-2025-58071	385553
CVE-2025-53868	385552
CVE-2025-54858	385563
CVE-2025-58096	385557
CVE-2025-53521	385564
CVE-2025-61958	385542
CVE-2025-61933	385558
CVE-2025-54854	385554
CVE-2025-61960	385545
CVE-2025-59481	385565
CVE-2025-61974	385551
CVE-2025-59483	385569
CVE-2025-54755	385549
CVE-2025-61990	385546

Please follow Qualys Threat Protection for more coverage on the latest vulnerabilities.

References

https://my.f5.com/manage/s/article/K000156572
https://my.f5.com/manage/s/article/K000154696
https://github.com/mandiant/brickstorm-scanner
https://cloud.google.com/blog/topics/threat-intelligence/brickstorm-espionage-campaign
https://www.cisa.gov/news-events/directives/ed-26-01-mitigate-vulnerabilities-f5-devices
https://www.bloomberg.com/news/articles/2025-10-16/potentially-catastrophic-breach-of-cyber-firm-blamed-on-china

---