Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

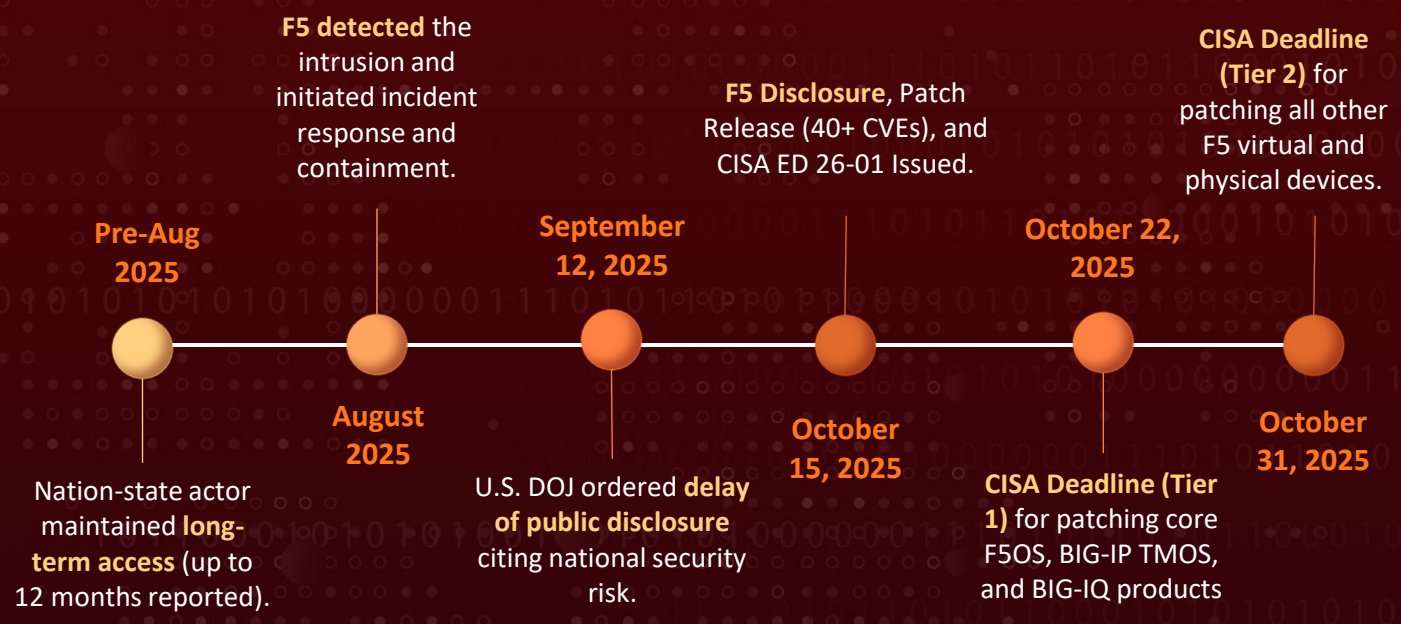
F5 BIG-IP Breach: Nation-State Hackers Expose Source Code and Undisclosed Flaws

Date of Publication	Admiralty Code	TA Number
October 17, 2025	A1	TA2025318

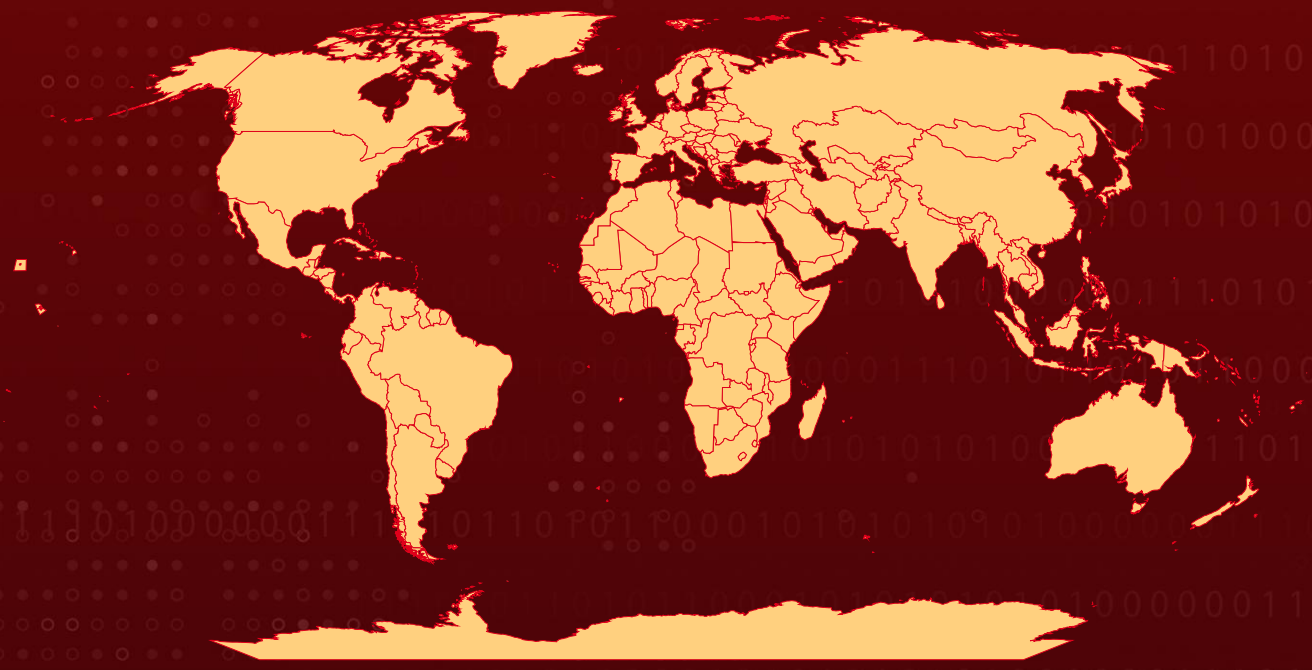
Summary

First Seen: August 2025
Targeted Countries: Worldwide
Targeted Platforms: F5 BIG-IP Product Development Environment and Engineering Knowledge Management Platforms
Threat Actor: Highly Sophisticated Nation-State Threat Actor
Attack: In August 2025, a highly sophisticated nation-state actor gained persistent access to F5's internal engineering and development systems, targeting BIG-IP, BIG-IQ, and F5OS platforms. The attackers exfiltrated source code, bug-tracking data, and undisclosed vulnerability information, including configuration details for a limited set of customers. With low confidence, it is suspected the operation is linked to the China-nexus espionage group UNC5221, associated with the BRICKSTORM malware family. While no active exploitation of vulnerabilities was observed, the breach underscores significant risks to enterprise and government networks relying on F5 technologies.

Incident Timeline



Attack Regions



Powered by Bing
© Australian Bureau of Statistics, GeoNames, Microsoft, Navinfo, Open Places, OpenStreetMap, TomTom, Zenrin

Attack Details

#1

In August 2025, F5 Networks discovered a significant cyber intrusion conducted by a highly sophisticated nation-state threat actor who maintained persistent access to its internal engineering and development systems. The attackers targeted F5's product development environments and knowledge management platforms, exfiltrating sensitive assets including BIG-IP source code, bug-tracking data, and details of undisclosed vulnerabilities. This breach poses substantial risk, as the stolen data may enable the development of targeted exploits against BIG-IP products widely deployed across enterprise and government networks.

#2 The compromise primarily affected F5's product development infrastructure rather than corporate business systems. Although F5 found no evidence of active exploitation at the time of detection, some exfiltrated files contained configuration details for a limited subset of customer deployments, which could increase potential exposure.

#3 F5 engaged cybersecurity partners, including IOActive, and NCC Group, to investigate and contain the intrusion. The company implemented enhanced security controls, rotated all relevant credentials and signing keys, and deployed expanded network monitoring to prevent further unauthorized access.

#4 Following containment, F5 released security updates addressing 44 vulnerabilities across BIG-IP, BIG-IQ, F5OS, and related modules. Notable CVEs include CVE-2025-53868 (Appliance-mode bypass), CVE-2025-58424 (TMM-level connection manipulation), CVE-2025-59483 (arbitrary file upload), and CVE-2025-61960 (APM portal denial-of-service).

#5 These issues encompass high-severity classes such as privilege escalation, input validation failures, and denial-of-service conditions. The U.S. Cybersecurity and Infrastructure Security Agency (CISA) issued Emergency Directive 26-01, mandating all federal agencies to identify, patch, and secure affected F5 systems by October 22 2025, underscoring the critical nature of the exposure.

#6 With low confidence, it is suspected that the breach is linked to a China-nexus espionage group tracked as UNC5221, associated with the BRICKSTORM malware family. The actor is assessed to have maintained access to F5 systems for approximately twelve months. This incident highlights the growing risk of supply-chain and vendor-infrastructure compromises targeting cybersecurity providers, with potential downstream consequences for both enterprise and government environments relying on F5 technologies.

Recommendations

Urgent Patching: Immediately inventory all F5 BIG-IP, BIG-IQ, F5OS, APM, and related modules in your environment and apply the October 15, 2025, security updates that patch over 44 critical vulnerabilities, including those linked to the breach. These patches remediate both known and undisclosed flaws potentially exposed by the attackers.

Access Hardening: Disable or restrict remote management interfaces that are not required and ensure multifactor authentication (MFA) is enabled on all administrative accounts to reduce risk of unauthorized access or credential abuse.

Network Monitoring and Threat Hunting: Employ enhanced network traffic monitoring, anomaly detection, and threat hunting focusing on unusual data exfiltration activity or suspicious logins, especially privilege escalation or access to source code repositories. Use endpoint detection and response (EDR) tools for early detection and response.

Decommission Unsupported Devices: Remove from service or isolate any F5 BIG-IP devices that have reached end of support to eliminate unpatchable attack surfaces. CISA's emergency directive mandates removal of vulnerable, unsupported systems from public networks.

Follow Regulatory and Advisory Guidance: Comply rigorously with CISA's Emergency Directive ED 26-01, including patch deadlines of October 22 for Tier 1 devices and October 31 for Tier 2. Report inventories and mitigation steps to appropriate governmental cybersecurity bodies as required.

Strengthen Software Supply Chain Security: Review the security posture of software development pipelines and engage third-party security assessments, as F5 did, to minimize risk of future insider or supply chain compromises.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	TA0002 Execution	TA0003 Persistence	TA0007 Discovery
TA0005 Defense Evasion	TA0040 Impact	TA0010 Exfiltration	TA0009 Collection
TA0006 Credential Access	TA0004 Privilege Escalation	T1548 Abuse Elevation Control Mechanism	T1548.002 Bypass User Account Control
T1078.003 Local Accounts	T1078 Valid Accounts	T1041 Exfiltration Over C2 Channel	T1005 Data from Local System
T1212 Exploitation for Credential Access	T1068 Exploitation for Privilege Escalation	T1083 File and Directory Discovery	T1498 Network Denial of Service
T1070 Indicator Removal	T1499 Endpoint Denial of Service	T1190 Exploit Public-Facing Application	T1003 OS Credential Dumping

CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2025-53868	F5 BIG-IP SCP and SFTP Appliance Mode Bypass Vulnerability	F5 BIG-IP SCP and SFTP OS	✗	✗	✓
CVE-2025-61955	F5 F5OS-A and F5OS-C Privilege Escalation Vulnerability	F5 F5OS-A and F5OS-C	✗	✗	✓
CVE-2025-57780	F5 F5OS-A and F5OS-C Privilege Escalation Vulnerability	F5 F5OS-A and F5OS-C	✗	✗	✓

Note: *F5 patched 44 vulnerabilities after a breach, no evidence of critical or RCE exploits. Patch links are hyperlinked to the tick marks.*

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2025-60016	F5 BIG-IP SSL/TLS Denial-of-Service Vulnerability	F5 BIG-IP SSL/TLS	✗	✗	✓
CVE-2025-48008	F5 BIG-IP MPTCP Denial-of-Service Vulnerability	F5 BIG-IP MPTCP	✗	✗	✓
CVE-2025-59781	F5 BIG-IP DNS Cache Denial-of-Service Vulnerability	F5 BIG-IP DNS Cache	✗	✗	✓
CVE-2025-41430	F5 BIG-IP SSL Orchestrator Denial-of-Service Vulnerability	F5 BIG-IP SSL Orchestrator	✗	✗	✓
CVE-2025-55669	F5 BIG-IP HTTP/2 Denial-of-Service Vulnerability	F5 BIG-IP HTTP/2	✗	✗	✓
CVE-2025-61951	F5 BIG-IP DTLS 1.2 Denial-of-Service Vulnerability	F5 BIG-IP DTLS 1.2	✗	✗	✓
CVE-2025-55036	F5 BIG-IP SSL Orchestrator Denial-of-Service Vulnerability	F5 BIG-IP SSL Orchestrator	✗	✗	✓
CVE-2025-54479	F5 BIG-IP PEM Denial-of-Service Vulnerability	F5 BIG-IP PEM	✗	✗	✓
CVE-2025-46706	F5 BIG-IP iRules Denial-of-Service Vulnerability	F5 BIG-IP iRules	✗	✗	✓
CVE-2025-59478	F5 BIG-IP AFM Denial-of-Service Vulnerability	F5 BIG-IP AFM	✗	✗	✓
CVE-2025-61938	F5 BIG-IP Advanced WAF and ASM Denial-of-Service Vulnerability	F5 BIG-IP Advanced WAF and ASM	✗	✗	✓
CVE-2025-54858	F5 BIG-IP Advanced WAF and ASM Denial-of-Service Vulnerability	F5 BIG-IP Advanced WAF and ASM	✗	✗	✓
CVE-2025-58120	F5 BIG-IP Next (CNF, SPK, Kubernetes) Denial-of-Service Vulnerability	F5 BIG-IP Next (CNF, SPK, Kubernetes)	✗	✗	✓
CVE-2025-53856	F5 BIG-IP TMM Denial-of-Service Vulnerability	F5 BIG-IP TMM	✗	✗	✓

Note: *F5 patched 44 vulnerabilities after a breach, no evidence of critical or RCE exploits. Patch links are hyperlinked to the tick marks.*

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2025-61974	F5 BIG-IP SSL/TLS Denial-of-Service Vulnerability)	F5 BIG-IP SSL/TLS	✗	✗	✓
CVE-2025-58071	F5 BIG-IP IPsec Denial-of-Service Vulnerability	F5 BIG-IP IPsec	✗	✗	✓
CVE-2025-53521	F5 BIG-IP APM Denial-of-Service Vulnerability	F5 BIG-IP APM	✗	✗	✓
CVE-2025-61960	F5 BIG-IP APM Denial-of-Service Vulnerability	F5 BIG-IP APM	✗	✗	✓
CVE-2025-54854	F5 BIG-IP APM Denial-of-Service Vulnerability	F5 BIG-IP APM	✗	✗	✓
CVE-2025-53474	F5 BIG-IP iRules Denial-of-Service Vulnerability	F5 BIG-IP iRules	✗	✗	✓
CVE-2025-61990	F5 BIG-IP TMM Denial-of-Service Vulnerability	F5 BIG-IP TMM	✗	✗	✓
CVE-2025-58096	F5 BIG-IP TMM Denial-of-Service Vulnerability	F5 BIG-IP TMM	✗	✗	✓
CVE-2025-61935	F5 BIG-IP Advanced WAF and ASM Denial-of-Service Vulnerability	F5 BIG-IP Advanced WAF and ASM	✗	✗	✓
CVE-2025-59778	F5 VELOS Denial-of-Service Vulnerability	F5 VELOS	✗	✗	✓
CVE-2025-59481	F5 BIG-IP iControl REST and tmsh Appliance Mode Bypass Vulnerability	F5 BIG-IP iControl REST and tmsh	✗	✗	✓
CVE-2025-61958	F5 BIG-IP tmsh Appliance Mode Bypass Vulnerability	F5 BIG-IP tmsh	✗	✗	✓
CVE-2025-47148	F5 BIG-IP APM and SSL Orchestrator Denial-of-Service Vulnerability	F5 BIG-IP APM and SSL Orchestrator	✗	✗	✓
CVE-2025-47150	F5 F5OS SNMP Denial-of-Service Vulnerability	F5 F5OS SNMP	✗	✗	✓

Note: *F5 patched 44 vulnerabilities after a breach, no evidence of critical or RCE exploits. Patch links are hyperlinked to the tick marks.*

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2025-55670	F5 BIG-IP Next (CNF, SPK, and Kubernetes) Denial-of-Service Vulnerability	F5 BIG-IP Next (CNF, SPK, and Kubernetes)	✗	✗	✓
CVE-2025-54805	F5 BIG-IP TMM Denial-of-Service Vulnerability	F5 BIG-IP TMM	✗	✗	✓
CVE-2025-59269	F5 BIG-IP Configuration utility XSS vulnerability	F5 BIG-IP Configuration utility	✗	✗	✓
CVE-2025-58153	F5 BIG-IP HSB Hardware Denial-of-Service Vulnerability	F5 BIG-IP Configuration utility	✗	✗	✓
CVE-2025-60015	F5 F5OS Out-of-Bounds Write Vulnerability	F5 F5OS	✗	✗	✓
CVE-2025-59483	F5 BIG-IP Configuration utility Arbitrary File Upload Vulnerability	F5 BIG-IP Configuration utility	✗	✗	✓
CVE-2025-60013	F5 F5OS-A FIPS HSM Password Appliance Mode Bypass Vulnerability	F5 F5OS-A FIPS HSM Password	✗	✗	✓
CVE-2025-59268	F5 BIG-IP Configuration utility Authentication Bypass Vulnerability	F5 BIG-IP Configuration utility	✗	✗	✓
CVE-2025-58474	F5 BIG-IP Advanced WAF/ASM and NGINX App Protect DNS lookup vulnerability	F5 BIG-IP Advanced WAF/ASM and NGINX	✗	✗	✓
CVE-2025-61933	F5 BIG-IP APM XSS vulnerability	F5 BIG-IP APM	✗	✗	✓
CVE-2025-54755	F5 BIG-IP Configuration utility Authentication Bypass Vulnerability	F5 BIG-IP Configuration utility	✗	✗	✓
CVE-2025-53860	F5 F5OS-A FIPS HSM Authentication Bypass Vulnerability	F5 F5OS-A FIPS HSM	✗	✗	✓
CVE-2025-58424	F5 BIG-IP TMM Data Corruption and Modification Vulnerability	F5 BIG-IP TMM	✗	✗	✓

Note: *F5 patched 44 vulnerabilities after a breach, no evidence of critical or RCE exploits. Patch links are hyperlinked to the tick marks.*

References

https://my.f5.com/manage/s/article/K000154696

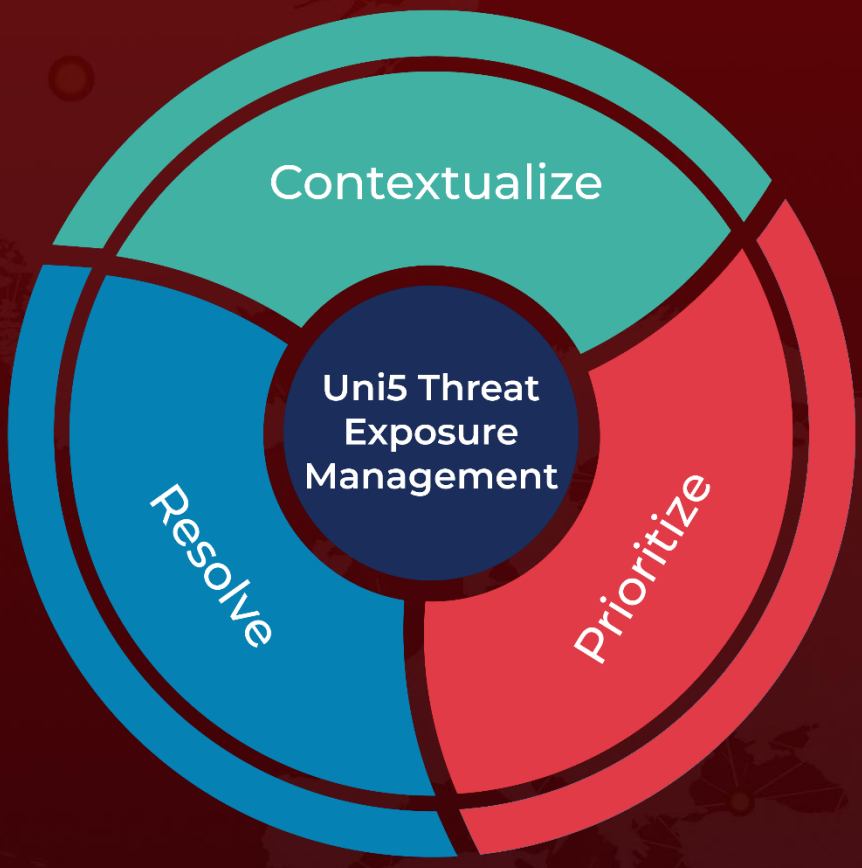
https://my.f5.com/manage/s/article/K000156572

https://www.cisa.gov/news-events/directives/ed-26-01-mitigate-vulnerabilities-f5-devices

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

October 17, 2025 . 4:30 AM

More at www.hivepro.com