Lowenstein Sandler

Client Alert

Data Privacy, Security, Safety & Risk Management

October 21, 2025

F5 Security Incident: BIG-IP Source Code Theft Spurs Urgent Actions

By Amy S. Mushahwar, Kathleen A. McGee, and Erich J. Kaletka

On October 15, application security vendor F5, Inc. disclosed that a highly sophisticated nation-state threat actor maintained long-term, persistent access to certain F5 systems. The attackers exfiltrated portions of BIG-IP[1] source code, internal documentation on undisclosed vulnerabilities, and some customer configuration and implementation data. Independent reviews confirm there is no evidence that the attackers tampered with F5's source code repositories, build and release pipelines, or software supply chain, and investigators (including Mandiant and CrowdStrike) found no indications that they accessed F5's customer databases, financial, support case management, or iHealth systems.

New Developments

Attribution: The intrusion has been attributed to a China-based espionage group (UNC5221) that leveraged a custom malware family known as BRICKSTORM to maintain persistence in F5's environment for over a year. This attribution underscores the sophistication and persistence of the threat actor involved.

CISA Emergency Mandate: In response to the incident, the Cybersecurity and Infrastructure Security Agency (CISA) issued Emergency Directive ED 26-01,[2] mandating that federal agencies immediately take inventory of all F5 BIG-IP devices, apply security patches by October 22 for core products and by October 31 for others, disconnect unsupported devices, and harden public-facing systems. Private sector organizations, especially those with government contracts, are strongly urged to follow the same guidance without delay.

Scope: The scope of the risk related to this incident is significant. Internet scans have identified more than 260,000 exposed F5 systems globally, with approximately 90% running BIG-IP Local Traffic Manager or Access Policy Manager (APM) modules, making them high-value targets for exploitation. Compounding this risk, F5's October security update introduced 44 new CVEs, including critical vulnerabilities such as CVE-2025-53868 (authentication bypass, CVSS 8.7) and CVE-2025-61955 and CVE-2025-57780 (privilege escalation, CVSS 8.8). These updates apply to BIG-IP, F5OS, BIG-IP Next for Kubernetes, BIG-IQ, and APM clients.

Why Does This Matter?

Given BIG-IP's role at the network edge for load balancing, firewalling, and traffic inspection, the theft of source code and vulnerability documentation creates an "imminent threat" to thousands of networks, including U.S. government agencies and Fortune 500 companies. While no active exploitation of undisclosed vulnerabilities has been confirmed, the risk of rapid exploitation, lateral movement, and potential supply chain attacks could be significant.

Immediate Actions for Enterprises

1. Apply all October 2025 patches immediately.
    - Prioritize BIG-IP, F5OS, BIG-IP Next, BIG-IQ, and APM clients.
2. Enable and monitor event streaming to SIEM.
    - Track admin logins, failed authentications, and configuration changes.
3. Use F5's hardening best practices.
    - Leverage iHealth automated checks and SIEM integration.

4. Validate signing certificates and trust anchors.
    - Ensure integrity of cryptographic trust chains.
5. Confirm managed service provider (MSP) and third-party compliance.
    - Verify that MSPs have applied all relevant updates.
6. Intensify threat hunting.
    - Look for anomalous authentication, configuration drift, and traffic patterns consistent with edge device exploitation.

Bottom Line

Although F5 has found no evidence of active exploitation to date, organizations should act with urgency. Applying patches promptly and maintaining rigorous monitoring are critical to reducing exposure and preventing potential follow-on attacks that could leverage information from this compromise. Every day a vulnerability remains unpatched increases the likelihood of exploitation.

For questions or assistance in responding to this incident, please contact the authors of this alert.

---

[1] *See*: https://www.f5.com/products/big-ip
[2] *See*: https://www.cisa.gov/news-events/directives/ed-26-01-mitigate-vulnerabilities-f5-devices

Contacts

Please contact the listed attorneys for further information on the matters discussed herein.

AMY S. MUSHAHWAR
Partner
Chair, Data, Privacy & Cybersecurity
T: 202.753.3825
amushahwar@lowenstein.com

KATHLEEN A. MCGEE
Partner
T: 646.414.6831
kmcgee@lowenstein.com

ERICH J. KALETKA
Associate
T: 862.926.2792
ekaletka@lowenstein.com
