# F5 Hit by Nation-State Attack – BIG-IP Code Theft Puts Federal and Public-Sector Networks at Risk

*A suspected Chinese state-backed group breached F5's internal systems, stealing source code and private vulnerability data tied to BIG-IP products.*

*The attackers maintained long-term access and exfiltrated technical files that could speed up zero-day development or patch bypasses. CISA issued an emergency directive warning of immediate threats to public-facing and federal networks using F5.*

*All organizations running BIG-IP should patch now and assume adversaries have detailed product insight.*

## Overview

F5 has disclosed that a suspected Chinese threat actor penetrated its development environment and exfiltrated portions of BIG-IP source code and undisclosed vulnerability data. The threat actor maintained persistent access for months before discovery, giving them a roadmap to identify zero-day flaws and target public infrastructure using F5 devices.

Of particular concern, some of the stolen files included configuration or implementation details tied to a subset of F5 customers, which could allow the threat actor to tailor exploits. Federal agencies and public-sector organizations are especially vulnerable in this case because many rely on F5 appliances to run public-facing systems (login portals, remote access gateways, and application delivery platforms). These systems are often connected directly to the internet, making them easy targets for nation-state attackers.

Attackers didn't just take source code; they also accessed internal vulnerability details. That gives them an advantage in uncovering new flaws or bypassing current patches, and it increases the likelihood of long-term access across government environments.

F5 is a major technology company focused on cybersecurity, cloud services, and application delivery networking. Its products are used by 48 of the Fortune 50 and serve over 23,000 customers across 170 countries. Review Aspire's recommendations below to reduce exposure and secure your environment.

## Aspire Protects

- **Patch** – Apply F5's latest patches for BIG-IP, F5OS, BIG-IP Next for Kubernetes, BIG-IQ, and APM clients. The company has provided guidance in their security advisory.
    - Ensure signing keys, certificates, and internal credentials have been rotated.
- List every deployed F5 device or component (BIG-IP, BIG-IQ, APM, DNS, SSL, etc.).
    - For each, check whether the management interface or admin ports are reachable from the public internet.
- Disable or restrict public access to management consoles. Permit only trusted IP ranges.
- Implement strict MFA and role-based access on F5 devices.
- Monitor and block cookie leak vectors if relevant (CISA flagged this in their directive).
- Track any exploit attempts that fit F5 code patterns (especially tied to source code knowledge).
- Deploy network filtering / monitoring on east-west traffic around F5 appliances.

### TTPs to Watch

Initial Access

- Exploit Public-Facing Application [T1190] – The attacker may exploit known or undisclosed BIG-IP vulnerabilities exposed to the internet to gain initial access.

Execution

- Command and Scripting Interpreter [T1059] – The attacker may run shell commands or scripts on compromised BIG-IP systems after access is gained.

Persistence

- Valid Accounts [T1078] – The attacker may create or leverage credentials to maintain access to BIG-IP admin interfaces or integrated systems.

Defense Evasion

- Obfuscated Files or Information [T1027] – The attacker may use custom or obfuscated payloads to avoid detection, especially when deploying post-exploit tooling.

### IoCs

There are no known IoCs at this time. Aspire is actively monitoring and will notify customers if any are found. For more details on how we can help protect your organization, contact Aspire's Customer Success Management team.

**Targeted Industries**

The F5 breach affects any organization using BIG-IP devices, but public-facing and federal systems are especially vulnerable due to exposure and high-value impact.

- Education
- Public Sector
- Finance
- Healthcare
- Legal
- Manufacturing
- Retail

## Aspire Service Offerings

- **Aspire Managed XDR (MXDR)**
  - Aspire Managed XDR (MXDR) combines next-generation eXtended Detection and Response (XDR) technology, a 24x7 security operations center (SOC), and the expertise of a US-based team of security professionals to identify and respond to threats across a broader attack surface.
  - Building on the existing capabilities of Managed Detection and Response (MDR), Aspire Managed XDR integrates and correlates telemetry from endpoints, network, cloud, email, identity, and more. This advanced platform creates valuable context enabling end-to-end visibility across all threat vectors.
  - Experienced security analysts and incident responders deliver 24x7 threat detection, analysis, and investigations – with both automated and human-led response actions to quickly mitigate cyber attacks.
- **Aspire Incident Response**
  - The ability to respond effectively to data breaches is critical to every organization. When attacks occur, IT leaders need a process that will ultimately maintain business continuity, protect the company reputation, and avoid fines, legal fees, and remediation costs.
  - Aspire offers incident response services to help you prepare for, manage, and recover from data breaches and network attacks. An experienced team uses industry-leading threat intelligence and the most current security technology to quickly respond to attacks, reduce damage, and minimize exposure.

## Supporting Documentation

Quarterly Security Notification (October 2025)

ED 26-01: Mitigate Vulnerabilities in F5 Devices | CISA

F5 Hack: Attack Linked to China, BIG-IP Flaws Patched, Governments Issue Alerts - SecurityWeek