Confirmed compromise of F5 network

The NCSC is advising organisations to follow the guidance issued by F5 and to install the latest security updates.

What has happened?

F5 has issued a statement reporting a compromise of its systems, and data exfiltration. This data is reported to include a portion of its BIG-IP source code and vulnerability information.

This access could enable a threat actor to:

- exploit F5 devices and software
- conduct static and dynamic analysis for identification of logical flaws and vulnerabilities as well as the ability to develop targeted exploits

Successful exploitation of the impacted F5 products could enable a threat actor to access embedded credentials and Application Programming Interface (API) keys, move laterally within an organisation's network, exfiltrate data, and establish persistent system access.

There is currently no indication that any customer networks have been impacted via the compromise of the F5 network.

While there is currently no suggestion that nginx has been affected, instances should always be updated to a latest version as per NCSC vulnerability management guidance.

Who is affected?

Affected F5 products:

- **Hardware:** BIG-IP iSeries, rSeries, or any other F5 device that has reached end of support
- **Software:** All devices running BIG-IP (F5OS), BIG-IP (TMOS), Virtual Edition (VE), BIG IP Next, BIG- IQ, and BIG-IP Next for Kubernetes (BNK) / Cloud-Native Network Functions (CNF)

What should I do?

If you use F5 products, you should take the following priority actions:

1. Identify all F5 products (hardware, software and virtualised).
2. Management interfaces should not be exposed to the internet. If an exposed management interface is found, a compromise assessment should be undertaken.
3. If you believe you have been compromised, you should contact F5 SIRT and, if you are in the UK, also report it to the NCSC.
4. Follow vendor best practice advice in Hardening your F5 system.
5. Install the latest F5 security updates.
6. Replace any product that have reached end of support or follow NCSC's obsolete products guidance.
7. Perform continuous network monitoring and threat hunting.

Further NCSC resources

The NCSC provides a range of free guidance, services and tools that help to secure systems.

- Follow NCSC guidance including vulnerability management, external attack surface management (EASM) buyer's guide and preventing lateral

movement.

- If your organisation is in the UK, you can sign up to the free NCSC Early Warning service to receive notifications of potential threats on your network.
- The NCSC Vulnerability Disclosure Toolkit helps organisations of all sizes with the essential components of implementing a vulnerability disclosure process.

PUBLISHED

15 October 2025

WRITTEN FOR

Public sector

Cyber security professionals

NEWS TYPE

Alert