|630 Freedom Business Center Drive, Suite 212|
|King of Prussia, PA 19406|
|610.768.1100|

F5 Security Incident – TS Partners Unaffected

Attestation: *TS Partners does not use F5 products or require F5 product(s) use by Clients.*

What Happened (Information-only / TSP does not use F5 products)

F5, Seattle-based maker of networking software, disclosed breach and reported:

Statements from F5:

"In August 2025, we learned a highly sophisticated nation-state threat actor maintained long-term, persistent access to, and downloaded files from, certain F5 systems. These systems included our BIG-IP product development environment and engineering knowledge management platforms."

"We have no evidence of modification to our software supply chain, including our source code and our build and release pipelines. This assessment has been validated through independent reviews by leading cybersecurity research firms NCC Group and IOActive."

"We have no evidence that the threat actor accessed or modified the NGINX source code or product development environment, nor do we have evidence they accessed or modified our F5 Distributed Cloud Services or Silverline systems."

"We have released updates for BIG-IP, F5OS, BIG-IP Next for Kubernetes, BIG-IQ, and APM clients. More information can be found in our October 2025 Quarterly Security Notification. We strongly advise updating to these new releases as soon as possible."

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

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

Additional information:

https://www.cisa.gov/news-events/alerts/2025/10/15/cisa-directs-federal-agencies-mitigate-vulnerabilities-f5-devices

For questions regarding Policy, contact CEO or COO

Last Review: October 16, 2025