مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

High- Severity Vulnerability in F5 BIG-IP

Tracking #:432316409

Date:18-10-2024

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a high-severity vulnerability in F5 BIG-IP that could be exploited to privilege escalation for authenticated users.

TECHNICAL DETAILS:

Vulnerability Details:

- **CVE-2024-45844-** High/8.6 (CVSS v4.0)
- BIG-IP monitor functionality may allow an authenticated attacker with at least Manager role privileges to elevate their privileges and/or modify the configuration.
- Impact:
  - Allows privilege escalation for authenticated users.
  - Compromises the control plane without exposing the data plane.
  - Classifies as CWE-306: Missing Authentication for Critical Function.

Product	Branch	Versions Known to be Vulnerable	Fixes introduced in
BIG-IP (all modules)	17.x	17.1.0 - 17.1.1	17.1.1.4
	16.x	16.1.0 - 16.1.4	16.1.5
	15.x	15.1.0 - 15.1.10	15.1.10.5

RECOMMENDATIONS:

- Upgrade all affected BIG-IP systems to the latest versions that include security patches.
- Conduct an audit of user roles and permissions, ensuring that only necessary personnel have Manager role access.
- Monitor system logs for unusual activities or unauthorized access attempts.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

- https://my.f5.com/manage/s/article/K000140061?utm_source=f5support&utm_medium=RSS