مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

High-Severity Vulnerability in F5 BIG-IP

Tracking #:432316458

Date:31-10-2024

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a high-severity vulnerability in F5 BIG-IP that could potentially be exploited, leading to denial-of-service conditions on affected systems.

TECHNICAL DETAILS:

Vulnerability Details:

- **CVE-2024-41996**
- CVSS v3 Base Score: 7.5 High
- A vulnerability has been identified in the Diffie-Hellman Key Exchange Protocol that could allow remote attackers to trigger unnecessary server-side calculations, potentially leading to resource exhaustion.
- By manipulating the order of public keys in the Diffie-Hellman Key Agreement Protocol, a remote attacker could induce the server to perform computationally expensive operations.
- Successful exploitation of this vulnerability could lead to:
    - **Resource Exhaustion:** Unnecessary server-side calculations could consume significant system resources.
    - **Denial of Service:** In severe cases, the server may become unresponsive or unable to handle legitimate traffic.

Product	Branch	Versions known to be vulnerable	Fixes introduced in	Vulnerable component or feature
BIG-IP (all modules)	17.x	17.1.0 - 17.1.1	None	**Control plane**: Configuration utility and OpenSSH ***Note**: Diffie-Hellman ciphers are not enabled by default in the Configuration utility but are enabled in the SSH server configuration.* **Data plane**: ClientSSL and ServerSSL profiles when configured with DHE ciphers. ***Note**: DHE ciphers are configured by default in ClientSSL and ServerSSL profiles.*
	16.x	16.1.0 - 16.1.5	None	
	15.x	15.1.0 - 15.1.10	None	

Mitigation:

To mitigate this vulnerability, it is recommended to disable Diffie-Hellman ciphers in BIG-IP configuration.

OpenSSH:

- OpenSSH allows Diffie-Hellman ciphers by default.
- To disable these ciphers:
    1. Log into the TMOS Shell (tmsh).
    2. Set the Security.CommonCriteria database key to true.

3. Reboot the BIG-IP system.

Note:

- Disabling Diffie-Hellman ciphers may impact connectivity. It is recommended to test changes in a non-production environment before deploying to production.
- For more information, please refer to the official F5 security advisories.

RECOMMENDATIONS:

The UAE Cyber Security Council recommends applying the mitigation or workaround provided by F5.

- Stay updated with the latest security advisories and patches from F5.

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/K000148343?utm_source=f5support&utm_medium=RSS