The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

TLP: WHITE

https://www.cisa.gov/tlp

Sources may use TLP:WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

DATE(S) ISSUED:

01/25/2022

SUBJECT:

A Vulnerability in F5Networks BIG-IP Could Allow for Denial of Service

OVERVIEW:

A vulnerability has been discovered in F5Networks BIG-IP, which could result in a denial-of-service (DoS). BIG-IP is a family of products covering software and hardware designed around application availability, access control, and security solutions. Successful exploitation of this vulnerability could allow an attacker to cause a denial of service to all servers sitting behind the BIG-IP system.

THREAT INTELLIGENCE:

There are currently no reports of this vulnerability being exploited in the wild.

SYSTEMS AFFECTED:

- F5 BIG-IP 12.1.6
- F5 BIG-IP 13.1.4
- F5 BIG-IP 14.1.0
- F5 BIG-IP 14.1.2.8
- F5 BIG-IP 14.1.3
- F5 BIG-IP 14.1.3.1
- F5 BIG-IP 14.1.4
- F5 BIG-IP 14.1.4.2
- F5 BIG-IP 14.1.4.3
- F5 BIG-IP 15.1.0
- F5 BIG-IP 15.1.0.5
- F5 BIG-IP 15.1.2
- F5 BIG-IP 15.1.3
- F5 BIG-IP 15.1.3.1

RISK:

Government:

- Large and medium government entities: **High**
- Small government: **Medium**

Businesses:

- Large and medium business entities: **High**

- Small business entities: **Medium**

Home users: Low

TECHNICAL SUMMARY:

A vulnerability has been discovered in F5Networks BIG-IP, which could result in a denial-of-service (DoS). This vulnerability exists when a FastL4 profile and an HTTP, FIX, and/or hash persistence profile are configured on the same virtual server, and undisclosed requests are received which can cause the virtual server to stop processing new client connections (CVE-2022-23027). Although this is a non-default configuration, FastL4 is a layer 4 profile to increase performance so having a FastL4 profile and a HTTP profile is likely not uncommon in deployments. The virtual server is utilized as a way to route connection over a certain port to specific servers so if the virtual server for port 80 or 443 was affected successful exploitation of this vulnerability could cause the impacted system to not allow any new client connections to webservers. Successful exploitation of this vulnerability could allow an attacker to cause a denial of service to all servers sitting behind the BIG-IP system.

RECOMMENDATIONS:

The following actions should be taken:

- Apply appropriate patches or appropriate mitigations provided by F5 to vulnerable systems immediately after appropriate testing.
- Deploy network intrusion detection systems to monitor network traffic to affected devices.

REFERENCES:

F5:

https://support.f5.com/csp/article/K30573026
https://techdocs.f5.com/kb/en-us/products/big-ip_ltm/manuals/product/ltm-basics-11-6-0/2.html
https://support.f5.com/csp/article/K09948701

CVE:

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-23027

TLP: WHITE

https://www.cisa.gov/tlp