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
www.cisa.gov/tlp
Information may be distributed without restriction, subject to standard copyright rules.

DATE(S) ISSUED:
05/05/2022
05/09/2022 – UPDATED
05/11/2022 - UPDATED

SUBJECT:
Multiple Vulnerabilities in F5Networks Products Could Allow for Arbitrary Code Execution

OVERVIEW:
Multiple vulnerabilities have been discovered in F5Networks products, the most severe of which could result in arbitrary code execution.

- BIG-IP is a family of products covering software and hardware designed around application availability, access control, and security solutions.
- Traffix SDC is a product that provides load balancing and gateway connectivity.
- Big-IQ Centralized Management tracks assets and manages policies for BIG-IP products.
- F5 Access for Android is an Android application that allows users to access enterprise networks and applications.
- BIG-IP Guided Configuration is a products that provides a way to deploy configurations of BIP-IP APM and Advanced WAF.
- The F5OS-A is the operating system software for the F5 rSeries system.
- NGINX Service Mesh is a product that allows for traffic control of distributed systems.
- BIG-IP APM provides access control and authentication for applications.

Successful exploitation of the most severe of these vulnerabilities could allow for arbitrary code execution. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than those who operate with administrative user rights.

THREAT INTELLIGENCE:
There are currently no reports of these vulnerabilities being exploited in the wild.

May 9 – UPDATED THREAT INTELLIGENCE:
BleepingComputer has released an article indicating that there are working exploits for CVE-2022-1388 out in the wild.

May 11 – UPDATED THREAT INTELLIGENCE:
CISA added CVE-2022-1388 to the KEV catalog on May 11, 2022 and continues to see open-source reporting of activity attempting to exploit these devices.

SYSTEMS AFFECTED:

- F5 BIG-IP 11.6.1 - 11.6.5
- F5 BIG-IP 12.1.0 - 12.1.6
- F5 BIG-IP 13.1.0 - 13.1.5
- F5 BIG-IP 14.1.0 - 14.1.4
- F5 BIG-IP 15.1.0 - 15.1.5
- F5 BIG-IP 16.1.0 - 16.1.2
- F5 Traffix SDC 5.1.0 – 5.2.0
- Big-IQ Centralized Management 8.0.0 -8.2.0
- Big-IQ Centralized Management 7.0.0 -7.1.0
- F5 F5OS-A 1.0.0
- F5 Access For Android 3.0.6 - 3.0.7
- NGINX Service Mesh 1.3.0 - 1.3.1
- BIG-IP Guided Configuration
- BIG-IP APM Clients 7.1.8 - 7.2.1

RISK:

Government:

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

Businesses:

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

Home users: Low

TECHNICAL SUMMARY:
Multiple vulnerabilities have been discovered in F5Networks products, the most severe of which could allow for remote code execution by an unauthenticated attacker with network access to the BIG-IP system through the management port and/or self IP addresses. Details of these vulnerabilities are as follows:

- A vulnerability in BIG-IP allows for remote code execution(CVE-2022-1388)
- A vulnerability in BIG-IP allows an authenticated user to run a limited set of commands (ping, traceroute, WOM diagnostics) (CVE-2022-1389)
- Multiple vulnerabilities in BIG-IP allow users to bypass Appliance mode restrictions (CVE-2022-25946, CVE-2022-27806, CVE-2022-26415)
- Multiple vulnerabilities in BIG-IP allow for XSS (CVE-2022-28707, CVE-2022-28716, CVE-2022-27878)
- Multiple vulnerabilities in BIG-IP allow for privilege escalation (CVE-2022-29263, CVE-2022-28714, CVE-2022-27634)
- Multiple vulnerabilities in BIG-IP allow for denial-of-service (CVE-2022-26372, CVE-2022-27189, CVE-2022-27230, CVE-2022-28691, CVE-2022-29491, CVE-2022-28705, CVE-2022-26890, CVE-2022-28701, CVE-2022-29473, CVE-2022-26370, CVE-2022-26517, CVE-2022-28706, CVE-2022-28708, CVE-2022-26130, CVE-2022-29480, CVE-2022-29479, CVE-2022-27182, CVE-2022-27181, CVE-2022-1468)
- A vulnerability in BIG-IP allows for a SAD DNS attack (CVE-2022-26071)
- A vulnerability in BIG-IP allows for remote code execution by a privileged, authenticated attacker (CVE-2022-28695)
- Multiple vulnerabilities in BIG-IP allow for authentication bypass (CVE-2022-28859, CVE-2022-27659, CVE-2022-26340)
- Multiple vulnerabilities in BIG-IP allow for information disclosure (CVE-2022-27636, CVE-2022-26835, CVE-2022-29474)
- A vulnerability in F5 Access for Android allows for information disclosure (CVE-2022-27875)
- A vulnerability in F5OS-A allows for information disclosure (CVE-2022-25990)
- A vulnerability in NGINX Service Mesh allows for authentication bypass that results in the attacker being able to affect traffic policies (CVE-2022-27495)
- Multiple vulnerabilities in Traffix SDC allow for XSS (CVE-2022-27662, CVE-2022-27880)
- Multiple vulnerabilities in BIG-IQ Centralized Management allows for authentication bypass (CVE-2022-26340)
- Multiple vulnerabilities in BIG-IQ Centralized Management allows for denial of service (CVE-2022-29479)
- A vulnerability in BIG-IP APM Clients allows for information disclosure (CVE-2022-27636)
- Multiple Vulnerabilities in BIG-IP APM Clients allow for privilege escalation (CVE-2022-28714, CVE-2022-29263)
- Multiple Vulnerabilities in BIG-IP Guided Configuration allow for XSS (CVE-2022-27878, CVE-2022-27230)
- Multiple vulnerabilities in BIG-IP Guided Configuration allow users to bypass Appliance mode restrictions (CVE-2022-25946, CVE-2022-27806)

Successful exploitation of the most severe of these vulnerabilities could allow for arbitrary code execution. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users

whose accounts are configured to have fewer user rights on the system could be less impacted than those who operate with administrative user rights.

RECOMMENDATIONS:
We recommend the following actions be taken:

- Apply appropriate patches or appropriate mitigations provided by F5 to vulnerable systems immediately after appropriate testing.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.
- Inform and educate users regarding the threats posed by hypertext links contained in emails or attachments especially from un-trusted sources.
- Apply the Principle of Least Privilege to all systems and services

May 11 – UPDATED RECOMMENDATIONS:
We recommend the following actions be taken:

- ***Vulnerability Scanning in your environment in order to ensure that remediation has occurred. CISA's Cyber Hygiene Services (CyHy) are free to all SLTTs, as well as public and private sector critical infrastructure organizations***
- ***Block all access to the iControl REST interface***
- ***Restrict iControl REST access***
- ***Modify BIG-IP httpd configuration***
- ***Run the bash script found in references in order to confirm if you are vulnerable***

REFERENCES:

F5:
https://support.f5.com/csp/article/K55879220

CVE:
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-1388
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-1389
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-1468
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-25946
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-25990
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-26071
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-26130
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-26340
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-26370
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-26372
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-26415
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-26517

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-26835
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-26890
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-27181
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-27182
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-27189
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-27230
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-27495
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-27634
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-27636
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-27659
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-27662
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-27806
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-27875
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-27878
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-27880
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-28691
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-28695
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-28701
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-28705
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-28706
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-28707
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-28708
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-28714
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-28716
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-28859
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-29263
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-29473
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-29474
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-29479
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-29480
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-29491

May 9 - UPDATED REFERENCES:
BleepingComputer:
https://www.bleepingcomputer.com/news/security/exploits-created-for-critical-f5-big-ip-flaw-install-patch-immediately/

May 11 – UPDATED REFERENCES:
CISA Cyber Hygiene Vulnerability Scanning:
https://www.cisa.gov/cyber-hygiene-services

CISA Known Exploited Vulnerabilities (KEV):
https://www.cisa.gov/known-exploited-vulnerabilities-catalog

Bash-Script to see if vulnerability exists in an F5 BIG-IP instance:
https://www.randori.com/blog/vulnerability-analysis-cve-2022-1388/