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
Disclosure is not limited. Subject to standard copyright rules, TLP: WHITE information may be distributed without restriction.
http://www.us-cert.gov/tlp/

DATE(S) ISSUED:
03/10/2021
03/20/2021 - UPDATED

SUBJECT:
Multiple Vulnerabilities in F5 BIG-IP and BIG-IQ Products Could Allow for Arbitrary Code Execution

OVERVIEW:
Multiple vulnerabilities have been discovered in F5 products, the most severe of which could allow for remote code execution.

- BIG-IP and BIG-IP Advanced WAF/ASM are a family of products covering software and hardware designed around application availability, access control, and security solutions.
- BIG-IQ enables administrators to centrally manage BIG-IP infrastructure across the IT landscape. It discovers, tracks, manages, and monitors physical and virtual BIG-IP devices - in the cloud, on premise, or co-located at your preferred datacenter.

Successful exploitation 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.

March 20 – UPDATED THREAT INTELLIGENCE:
Multiple security vendors have observed mass scanning and successful exploitation of CVE-2021-22986, which allows for unauthenticated remote code execution. The Mirai Botnet has been observed exploiting vulnerabilities highlighted in this advisory as well. Please review the reference from NCC Group for detecting IOCs.

SYSTEMS AFFECTED:
- BIG-IP (All modules) prior to version 16.0.1.1
- BIG-IQ prior to version 8.0.0
- BIG-IP Advanced WAF/ASM prior to version 16.0.1.1

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 F5 products, the most severe of which could allow for remote code execution. The details of the vulnerabilities are as follows:

- iControl REST unauthenticated remote command execution vulnerability (CVE-2021-22986)
    - This vulnerability allows for unauthenticated attackers with network access to the iControl REST interface, through the BIG-IP management interface and self IP addresses, to execute arbitrary system commands, create or delete files, and disable services. This vulnerability can only be exploited through the control plane and cannot be exploited through the data plane. Exploitation can lead to complete system compromise. The BIG-IP system in Appliance mode is also vulnerable.
- Appliance mode TMUI authenticated remote command execution vulnerability (CVE-2021-22987)
    - This vulnerability allows authenticated users with network access to the Configuration utility, through the BIG-IP management port, or self IP addresses, to execute arbitrary system commands, create or delete files, or disable services. This vulnerability can only be exploited through the control plane and cannot be exploited through the data plane. Exploitation can lead to complete system compromise and breakout of Appliance mode. Appliance mode is enforced by a specific license or may be enabled or disabled for individual vCMP guest instances.
- TMUI authenticated remote command execution vulnerability (CVE-2021-22988)
    - This vulnerability allows authenticated users with network access to the Configuration utility, through the BIG-IP management port or self IP addresses, to execute arbitrary system commands, create or delete files, or disable services. This vulnerability can only be exploited through the control plane and cannot be exploited through the data plane. Exploitation can lead to complete system compromise.
- Advanced WAF/ASM TMUI authenticated remote command execution vulnerability (CVE-2021-22989)
    - This vulnerability allows highly privileged authenticated users with the roles Administrator, Resource Administrator, or Application Security Administrator with network access to the Configuration utility, through the BIG-IP management port or self IP addresses, to execute arbitrary system commands, create or delete files, or disable services. This vulnerability can only be exploited through the control plane and cannot be exploited through the data plane. Exploitation can lead to complete system compromise and breakout of Appliance mode. Appliance mode is enforced by a specific license or may be enabled or disabled for individual vCMP guest instances.

- Advanced WAF/ASM TMUI authenticated remote command execution vulnerability (CVE-2021-22990)
    - This vulnerability allows highly privileged authenticated users with the roles Administrator, Resource Administrator, or Application Security Administrator with network access to the Configuration utility, through the BIG-IP management port or self IP addresses, to execute arbitrary system commands, create and delete files, or disable services. This vulnerability can only be exploited through the control plane and cannot be exploited through the data plane. Exploitation can lead to complete system compromise.
- TMM buffer-overflow vulnerability (CVE-2021-22991)
    - This vulnerability affects systems with one or more of the following configurations:
        - BIG-IP APM - A virtual server associated with a BIG-IP APM profile. All BIG-IP APM use cases are vulnerable.
        - BIG-IP ASM - Only BIG-IP ASM Risk Engine use cases are vulnerable. BIG-IP ASM Risk Engine is currently available to Early Access customers only and requires a special license.
        - BIG-IP PEM - This vulnerability affects BIG-IP systems with the following configuration:
            - The system has an active license for URL Filtering.
                - One or more virtual servers uses URL categorization through one of the following:
                    - An iRule
                    - A local traffic policy
                    - A BIG-IP PEM policy
        - Secure Web Gateway (SWG) - URL categorization is fundamental to the operation of SWG. All SWG use cases are vulnerable. SWG requires a separate subscription.
        - SSL Orchestrator - Use of the SSL Orchestrator Categorization macro exposes this vulnerability.
        - BIG-IP system - A virtual server associated with an HTTP and a local traffic policy that has a rule condition with the HTTP URI or HTTP Referer and Use normalized URI options enabled (the Use normalized URI option is disabled by default). This vulnerability can only be exploited through the data plane and cannot be exploited through the control plane. Exploitation can lead to complete system compromise.
- Advanced WAF/ASM buffer-overflow vulnerability (CVE-2021-22992)
    - A sophisticated attacker must have control over the back-end web servers (pool members) or the ability to manipulate the server-side HTTP responses to the virtual server to exploit this vulnerability. With this level of back-end control, the attacker may cause the BIG-IP Advanced WAF/ASM system to experience a denial-of-service (DoS). In the worst case, the attacker may execute arbitrary code on the BIG-IP Advanced WAF/ASM system. This vulnerability can only be exploited through the data plane and cannot be exploited through the control plane. Exploitation can lead to complete system compromise.

Successful exploitation 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:
The following actions should 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 rights) to diminish the effects of a successful attack.
- Apply the Principle of Least Privilege to all systems and services.

March 20 – UPDATED RECOMMENDATIONS:

- ***Restrict access to the management interface for authorized hosts only.***

REFERENCES:
F5:
https://support.f5.com/csp/article/K02566623
https://support.f5.com/csp/article/K03009991
https://support.f5.com/csp/article/K18132488
https://support.f5.com/csp/article/K70031188
https://support.f5.com/csp/article/K56142644
https://support.f5.com/csp/article/K45056101
https://support.f5.com/csp/article/K56715231
https://support.f5.com/csp/article/K52510511

CVE:
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-22986
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-22987
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-22988
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-22989
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-22990
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-22991
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-22992

March 20 – UPDATED REFERENCES
NCC Group:
https://research.nccgroup.com/2021/03/18/rift-detection-capabilities-for-recent-f5-big-ip-big-ig-icontrol-rest-api-vulnerabilities-cve-2021-22986/