JOINT CYBERSECURITY ADVISORY

Coauthored by:

TLP:WHITE

Product ID: AA22-138A

May 18, 2022

MS-ISAC®
Multi-State Information
Sharing & Analysis Center®

Threat Actors Exploiting F5 BIG-IP CVE-2022-1388

SUMMARY

The Cybersecurity and Infrastructure Security Agency (CISA) and the Multi-State Information Sharing & Analysis Center (MS-ISAC) are releasing this joint Cybersecurity Advisory (CSA) in response to active exploitation of CVE-2022-1388. This recently disclosed vulnerability in certain versions of F5 Networks, Inc., (F5) BIG-IP enables an unauthenticated actor to gain control of affected systems via the management port or self-IP addresses.

F5 released a patch for CVE-2022-1388 on May 4, 2022, and proof of concept (POC) exploits have since been publicly released, enabling less sophisticated actors to exploit the vulnerability. Due to previous exploitation of F5 BIG-IP vulnerabilities, CISA and MS-ISAC assess unpatched F5 BIG-IP devices are an attractive target; organizations that have not applied the patch are vulnerable to actors taking control of their systems.

According to public reporting, there is active exploitation of this vulnerability, and CISA and MS-ISAC expect to see widespread exploitation of unpatched F5 BIG-IP devices (mostly with publicly exposed management ports or self IPs) in both government and private sector networks. CISA and MS-ISAC strongly urge users and administrators to remain aware of the ramifications of exploitation and use the recommendations in this CSA—including upgrading their software to fixed versions—to help secure their organization's systems against malicious cyber operations. Additionally, CISA and MS-ISAC strongly encourage administrators to deploy the signatures included in this CSA to help determine whether their systems have been compromised. CISA and MS-ISAC especially encourage organizations who did not patch immediately or whose F5 BIG-IP device management interface has been exposed to the internet to assume compromise and hunt for malicious activity using the detection signatures in this CSA. If potential compromise is detected, organizations should apply the incident response recommendations included in this CSA.

Actions for administrators to take today:

- Do not expose management interfaces to the internet.
- Enforce multi-factor authentication.
- Consider using CISA's Cyber Hygiene Services.

TECHNICAL DETAILS

CVE-2022-1388 is a critical iControl REST authentication bypass vulnerability affecting the following versions of F5 BIG-IP:[1]

- 16.1.x versions prior to 16.1.2.2
- 15.1.x versions prior to 15.1.5.1
- 14.1.x versions prior to 14.1.4.6
- 13.1.x versions prior to 13.1.5
- All 12.1.x and 11.6.x versions

An unauthenticated actor with network access to the BIG-IP system through the management port or self IP addresses could exploit the vulnerability to execute arbitrary system commands, create or delete files, or disable services. F5 released a patch for CVE-2022-1388 for all affected versions—except 12.1.x and 11.6.x versions—on May 4, 2022 (12.1.x and 11.6.x versions are end of life [EOL], and F5 has stated they will not release patches).[2]

POC exploits for this vulnerability have been publicly released, and on May 11, 2022, CISA added this vulnerability its Known Exploited Vulnerabilities Catalog, based on evidence of active exploitation. Due to the POCs and ease of exploitation, CISA and MS-ISAC expect to see widespread exploitation of unpatched F5 BIG-IP devices in government and private networks.

DETECTION METHODS

CISA recommends administrators, especially of organizations who did not immediately patch, to:

- See the F5 Security Advisory K23605346 for indicators of compromise.
- See the F5 guidance K11438344 if you suspect a compromise.
- Deploy the following CISA-created Snort signature:

```
alert tcp any any -> any $HTTP_PORTS (msg:”BIG-IP F5 iControl:HTTP POST URI
‘/mgmt./tm/util/bash’ and content data ‘command’ and ‘utilCmdArgs’:CVE-
2022-1388”; sid:1; rev:1; flow:established,to_server;
flowbits:isnotset,bigip20221388.tagged; content:”POST”; http_method;
content:”/mgmt/tm/util/bash”; http_uri; content:”command”;
http_client_body; content:”utilCmdArgs”; http_client_body;
flowbits:set,bigip20221388.tagged; tag:session,10,packets; reference:cve-
2022-1388; reference:url,github.com/alt3kx/CVE-2022-1388_PoC; priority:2;
metadata:service http;)
```

Additional resources to detect possible exploitation or compromise are identified below:

- Emerging Threats suricata signatures. **Note:** CISA and MS-ISAC have verified these signatures are successful in detection of both inbound exploitation attempts (SID: 2036546) as well as post exploitation, indicating code execution (SID: 2036547).

  - SID 2036546

```
alert http $HOME_NET any -> $EXTERNAL_NET any (msg:"ET EXPLOIT F5 BIG-
IP iControl REST Authentication Bypass (CVE 2022-1388) M1";
flow:established,to_server; content:"POST"; http_method;
content:"/mgmt/tm/util/bash"; http_uri; fast_pattern;
content:"Authorization|3a 20|Basic YWRtaW46"; http_header;
content:"command"; http_client_body; content:"run"; http_client_body;
distance:0; content:"utilCmdArgs"; http_client_body; distance:0;
http_connection; content:"x-F5-Auth-Token"; nocase; http_header_names;
content:!"Referer"; content:"X-F5-Auth-Token";
flowbits:set,ET.F5AuthBypass; reference:cve,2022-1388;
classtype:trojan-activity; sid:2036546; rev:2; metadata:attack_target
Web_Server, created_at 2022_05_09, deployment Perimeter, deployment
SSLDecrypt, former_category EXPLOIT, performance_impact Low,
signature_severity Major, updated_at 2022_05_09;)
```

  - SID 2036547

```
alert http $HOME_NET any -> any any (msg:"ET EXPLOIT F5 BIG-IP
iControl REST Authentication Bypass Server Response (CVE 2022-1388)";
flow:established,to_client; flowbits:isset,ET.F5AuthBypass;
content:"200"; http_stat_code; file_data; content:"kind";
content:"tm|3a|util|3a|bash|3a|runstate"; fast_pattern; distance:0;
content:"command"; distance:0; content:"run"; distance:0;
content:"utilCmdArgs"; distance:0; content:"commandResult";
distance:0; reference:cve,2022-1388; classtype:trojan-activity;
sid:2036547; rev:1; metadata:attack_target Web_Server, created_at
2022_05_09, deployment Perimeter, deployment SSLDecrypt,
former_category EXPLOIT, performance_impact Low, signature_severity
Major, updated_at 2022_05_09;)
```

- Palo Alto Networks Unit 42 Threat Brief: CVE-2022-1388. This brief includes indicators of compromise. **Note:** due to the urgency to share this information, CISA and MS-ISAC have not yet validated this content.
- Cisco Talos Intelligence Group - Comprehensive Threat Intelligence: Threat Advisory: Critical F5 BIG-IP Vulnerability. This blog includes indicators of compromise. **Note:** due to the urgency to share this information, CISA and MS-ISAC have not yet validated this content.
- Randori's bash script. This script can be used to identify vulnerable instances of BIG-IP. **Note:** MS-ISAC has verified this bash script identifies vulnerable instances of BIG-IP.

INCIDENT RESPONSE

If an organization's IT security personnel discover system compromise, CISA and MS-ISAC recommend they:

1. **Quarantine or take offline potentially affected hosts.**
2. **Reimage compromised hosts.**
3. **Provision new account credentials.**
4. **Limit access to the management interface** to the fullest extent possible.
5. **Collect and review artifacts** such as running processes/services, unusual authentications, and recent network connections.
6. **Report the compromise** to CISA via CISA's 24/7 Operations Center (report@cisa.gov or 888-282-0870). State, local, tribal, or territorial government entities can also report to MS-ISAC (SOC@cisecurity.org or 866-787-4722).

See the joint CSA from the cybersecurity authorities of Australia, Canada, New Zealand, the United Kingdom, and the United States on Technical Approaches to Uncovering and Remediating Malicious Activity for additional guidance on hunting or investigating a network, and for common mistakes in incident handling. CISA and MS-ISAC also encourage government network administrators to see CISA's Federal Government Cybersecurity Incident and Vulnerability Response Playbooks. Although tailored to federal civilian branch agencies, these playbooks provide operational procedures for planning and conducting cybersecurity incident and vulnerability response activities and detail steps for both incident and vulnerability response.

MITIGATIONS

CISA and MS-ISAC recommend organizations:

- Upgrade F5 BIG-IP software to fixed versions; organizations using versions 12.1.x and 11.6.x should upgrade to supported versions.
- If unable to immediately patch, implement F5's temporary workarounds:
    - Block iControl REST access through the self IP address.
    - Block iControl REST access through the management interface.
    - Modify the BIG-IP httpd configuration.

See F5 Security Advisory K23605346 for more information on how to implement the above workarounds.

CISA and MS-ISAC also recommend organizations apply the following best practices to reduce risk of compromise:

- Maintain and test an incident response plan.
- Ensure your organization has a vulnerability program in place and that it prioritizes patch management and vulnerability scanning. **Note:** CISA's Cyber Hygiene Services (CyHy) are free to all SLTT organizations and public and private sector critical infrastructure organizations: https://www.cisa.gov/cyber-hygiene-services.

- Properly configure and secure internet-facing network devices.
  - Do not expose management interfaces to the internet.
  - Disable unused or unnecessary network ports and protocols.
  - Disable/remove unused network services and devices.
- Adopt zero-trust principles and architecture, including:
  - Micro-segmenting networks and functions to limit or block lateral movements.
  - Enforcing multifactor authentication (MFA) for all users and VPN connections.
  - Restricting access to trusted devices and users on the networks.

REFERENCES

[1] K23605346: BIG-IP iControl REST vulnerability CVE-2022-1388

[2] K11438344: Considerations and guidance when you suspect a security compromise on a BIG-IP system