CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY CISA

America’s Cyber Defense Agency

NATIONAL COORDINATOR FOR CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE

CYBERSECURITY ADVISORY

Threat Actor Exploitation of F5 BIG-IP CVE-2020-5902

Last Revised: July 24, 2020 **Alert Code:** AA20-206A

Give Feedback

Summary

The Cybersecurity and Infrastructure Security Agency (CISA) is issuing this alert in response to recently disclosed exploits that target F5 BIG-IP devices that are vulnerable to CVE-2020-5902. F5 Networks, Inc. (F5) released a patch for CVE-2020-5902 on June 30, 2020.[1] <https://support.f5.com/csp/article/k52145254> Unpatched F5 BIG-IP devices are an attractive target for malicious actors. Affected organizations that have not applied the patch to fix this critical remote code execution (RCE) vulnerability risk an attacker exploiting CVE-2020-5902 to take control of their system. **Note:** F5’s security advisory for CVE-2020-5902 states that there is a high probability that any remaining unpatched devices are likely already compromised.

CISA expects to see continued attacks exploiting unpatched F5 BIG-IP devices and strongly urges users and administrators to upgrade their software to the fixed versions. CISA also advises that administrators deploy the signature included in this Alert to help them determine whether their systems have been compromised.

This Alert also provides additional detection measures and mitigations for victim organizations to help recover from attacks resulting from CVE-2020-5902. CISA encourages administrators to remain aware of the ramifications of exploitation and to use the recommendations in this alert to help secure their organization's systems against attack.

Background

CISA has conducted incident response engagements at U.S. Government and commercial entities where malicious cyber threat actors have exploited CVE-2020-5902—an RCE vulnerability in the BIG-IP Traffic Management User Interface (TMUI)—to take control of victim systems. On June 30, F5 disclosed CVE-2020-5902, stating that it allows attackers to, "execute arbitrary system commands, create or delete files, disable services, and/or execute arbitrary Java code."

On July 4, open-source reporting indicated a proof-of-concept code was available and threat actors were exploiting the vulnerability by attempting to steal credentials. On July 5 security researchers posted exploits that would allow threat actors to exfiltrate data or execute commands on vulnerable devices. The risk posed by the vulnerability is critical.

Give Feedback

Technical Details

CISA has observed scanning and reconnaissance, as well as confirmed compromises, within a few days of F5's patch release for this vulnerability. As early as July 6, 2020, CISA has seen broad scanning activity for the presence of this vulnerability across federal departments and agencies—this activity is currently occurring as of the publication of this Alert.

CISA has been working with several entities across multiple sectors to investigate potential compromises relating to this vulnerability. CISA has confirmed two compromises and is continuing to investigate. CISA will update this Alert with any additional actionable information.

Detection Methods

CISA recommends administrators see the F5 Security Advisory K52145254 for indicators of compromise and F5's CVE-2020-5902 IoC Detection Tool.[2] <https://support.f5.com/csp/article/k52145254> CISA also recommends organizations complete the following actions in conducting their hunt for this exploit:

- Quarantine or take offline potentially affected systems
- Collect and review artifacts such as running processes/services, unusual authentications, and recent network connections
- Deploy the following CISA-created Snort signature to detect malicious activity:

```
alert tcp any any -> any $HTTP_PORTS (msg:"BIG-IP:HTTP URI
GET contains '/tmui/login.jsp/..|3b|/tmui/':CVE-2020-5902";
sid:1; rev:1; flow:established,to_server;
content:"/tmui/login.jsp/..|3b|/tmui/"; http_uri;
fast_pattern:only; content:"GET"; nocase; http_method;
priority:2; reference:url,github.com/yassineaboukir/CVE-
2020-5902; reference:cve,2020-5902; metadata:service http;)
```

Give Feedback

Mitigations

CISA strongly urges organizations that have not yet done so to upgrade their BIG-IP software to the corresponding patches for CVE-2020-5902. If organizations detect evidence of CVE-2020-5902 exploitation after patching and applying the detection measures in this alert, CISA recommends taking immediate action to reconstitute affected systems.

Should an organization's IT security personnel discover system compromise, CISA recommends they:

- Reimage compromised hosts
- Provision new account credentials
- Limit access to the management interface to the fullest extent possible
- Implement network segmentation
  - **Note:** network segmentation is a very effective security mechanism to help prevent an intruder from propagating exploits or laterally moving within an internal network. Segregation separates network segments based on role and functionality. A securely segregated network can limit the spread of malicious occurrences, reducing the impact from intruders that gain a foothold somewhere inside the network.

Contact Information

Recipients of this report are encouraged to contribute any additional information that they may have related to this threat. For any questions related to this report, please contact CISA at

- Phone: 1-844-Say-CISA (1-844-729-2472)
- Email: central@cisa.dhs.gov

References

[1] F5 Security Advisory K52145254 <https://support.f5.com/csp/article/k52145254>
[2] F5 Security Advisory K52145254 <https://support.f5.com/csp/article/k52145254>
CISA Factsheet: Guidance for F5 BIG-IP TMUI Vulnerability (CVE-2020-5902) <https://www.cisa.gov/publication/guidance-f5-big-ip-vulnerability-fact-sheet>

Revisions

July 24, 2020: Initial Version

This product is provided subject to this Notification </notification> and this Privacy & Use </privacy-policy> policy.

Please share your thoughts

We recently updated our anonymous product survey; we welcome your feedback.

Return to top

Topics </topics> **Spotlight** </spotlight> **Resources & Tools** </resources-tools>

News & Events </news-events> **Careers** </careers> **About** </about>

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

CISA Central

1-844-Say-CISA contact@cisa.dhs.gov

Give Feedback

CISA.gov
An official website of the U.S. Department of Homeland Security

About CISA </about>

Budget and Performance <https://www.dhs.gov/performance-financial-reports>

DHS.gov <https://www.dhs.gov>

FOIA Requests <https://www.dhs.gov/foia>

No FEAR Act </no-fear-act>

Office of Inspector General <https://www.oig.dhs.gov/>

Privacy Policy </privacy-policy>

Subscribe

The White House <https://www.whitehouse.gov/>

Give Feedback