IT Security | Supply Chain | OT Security | Insider Threat | Physical Security | Interoperable Communications

GUIDANCE FOR F5 BIG-IP TRAFFIC MANAGEMENT USER INTERFACE VULNERABILITY (CVE-2020-5902)

JULY 24, 2020

AT-A-GLANCE RECOMMENDATIONS

- ✓ Install F5 BIG-IP updated, fixed version
- ✓ Conduct incident investigation
- ✓ Implement mitigation recommendations
- ✓ Consider third-party incident response support

THE PROBLEM

On June 30, F5 disclosed a remote code execution (RCE) vulnerability in the BIG-IP Traffic Management User Interface (TMUI) that allows for file system manipulation and arbitrary code execution. The vulnerability allows an attacker to read the `/etc./passwd` file, and also to run arbitrary commands in the BIG-IP command shell/environment. The exploit is straightforward.

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. The next day, 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.

Audience and Scope

- This guidance is intended to advise critical infrastructure administrators and network defenders on the critical risk posed by a remote code execution (RCE) vulnerability in the F5 BIG-IP Traffic Management User Interface (TMUI).
- The vulnerability allows for an attacker to take control of an affected system to conduct file system manipulation and arbitrary code execution.
- Entities whose management interface was exposed to the internet should assume a compromise has occurred and conduct appropriate hunt and incident response activities.
- Business and government executive leaders should be aware if this critical vulnerability exists on their networks and assess their plan to address this specific, significant risk.

RECOMMENDED ACTIONS

The Cybersecurity and Infrastructure Security Agency (CISA) advises all BIG-IP users to update their devices to the F5 fixed software version as soon as possible. **However, users and administrators whose BIG-IP TMUI was exposed to the internet** should assume they were compromised and take immediate action to reconstitute affected systems.

Install F5 BIG-IP updated version

F5 released a security advisory to address the vulnerability—CVE-2020-5902—in the BIG-IP TMUI. Users and administrators should review the F5 advisory for CVE-2020-5902 and upgrade to the appropriate version.

Conduct incident investigation

An incident investigation or "hunt" on a network should encompass the review of a broad variety of artifacts to identify any suspicious activity that may be related to an F5 BIG-IP exploit.

For this exploit, CISA recommends that organizations:

- quarantine or take offline affected systems;
- collect and review artifacts such as running processes/services, unusual authentications, and recent network connections; and
- deploy the CISA-created Snort signature to detect malicious activity that is in CISA Activity Alert (AA20-206A).

Implement mitigation recommendations

Properly implemented defensive techniques and programs make it more difficult for a threat actor to gain access to a network and remain persistent yet undetected.

After conducting a hunt for this exploit, CISA recommends that organizations:

- reimage compromised hosts,
- provision new account credentials, and
- limit access to the management interface to the fullest extent possible.

Proper network segmentation is a very effective security mechanism to 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 contain malicious occurrences, reducing the impact from intruders in the event that they have gained a foothold somewhere inside the network.**

Consider third-party incident response support

For some organizations, incident response support from a third-party IT security organization can help properly handle the incident response, ensure that the actor is eradicated from the network, and avoid residual issues that could result in follow-up compromises once the incident is closed.

HELPFUL LINKS AND REFERENCE MATERIALS

1. CISA Tip: Handling Destructive Malware
2. CISA Tip: Securing Network Infrastructure Devices
3. CISA Activity Alert (AA20-206A): Threat Actor Exploitation of F5 BIG IP