Serianu Cyber Security Advisory

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

Serianu SOC Advisory Number:

TA – 2020/004

Date(s) issued:

5th August 2020

Systems Affected

- F5 BIG-IP devices

OVERVIEW:

Serianu research team has identified exploits that target F5 BIG-IP devices that are vulnerable to CVE-2020-5902.F5 networks released a patch for CVE-2020-5902 on June 30, 2020. 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.

Serianu research team 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. We advise administrators to deploy signatures to help them determine whether their systems have been compromised. We also encourage administrators to remain aware of the implications of exploitation and to use the recommendations in this alert to help secure their organization's systems against attack.

Description of Attack

Serianu has conducted investigations pertaining to this vulnerability where malicious cyber threat actors have exploited CVE-2020-5902 an RCE vulnerability in the BIG-IP Traffic Management User Interface (TMUI). This vulnerability allows attackers to execute arbitrary system commands, create or delete files, disable services and execute arbitrary Java code.

In recent incidents, malicious attackers are exploiting the vulnerability by attempting to steal credentials. Serianu researchers identified that this exploits would allow threat actors to exfiltrate data or execute commands on vulnerable devices. The risk posed by the vulnerability is critical. In addition, the attack metrics have been found scanning and reconnaissance on the F5s patched released vulnerability. Serianu research team will continue further to investigation this vulnerability.

Detection Methods

Serianu recommends organizations to complete the following actions in conducting their threat 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 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,202

Recommendations and Counter Measures

Serianu 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:

Serianu recommends the following as a mitigation procedure;

- Reimage compromised hosts.
- Provision of new account credentials.
- Limit access to the management interface to the fullest extent possible.
- Implement network segmentation: This 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.

Information Sharing

As a means of preventing such attacks from occurring, we encourage any organisation or individual that has access to threat actor exploitations share it with us through our email: info@serianu.com.