Cybersecurity news: F5 releases an RCE vulnerability fix



ARTICLE 07.06.20 DEAN DORTON

Over the holiday weekend, F5 released a fix for a vulnerability discovered that allows remote code execution and file access under certain configurations. In the most dire configurations, the F5 Traffic Management User Interface (TMUI) is publicly accessible and subject to direct exploit. Starting July 4, there are reports this issue is being actively exploited in the wild; successful exploit of this issue results in complete compromise of F5, and could allow threat actors to traverse hard security boundaries (external to internal or external to dmz).

Security Advisory Description

In BIG-IP versions 15.0.0-15.1.0.3, 14.1.0-14.1.2.5, 13.1.0-13.1.3.3, 12.1.0-12.1.5.1, and 11.6.1-11.6.5.1, the Traffic Management User Interface (TMUI), also referred to as the Configuration utility, has a Remote Code Execution (RCE) vulnerability in undisclosed pages. (Read more: CVE-2020-5902)

Impact

According to F5, this vulnerability allows for unauthenticated attackers, or authenticated users, with network access to the TMUI, through the BIG-IP management port and/or Self IPs, to execute arbitrary system commands, create or delete files, disable services, and/or execute arbitrary Java code. This vulnerability may result in complete system compromise. The BIG-IP system in Appliance mode is also vulnerable. This issue is not exposed on the data plane; only the control plane is affected.

CVE

10.0 (this is the highest possible rating for a vulnerability – meaning it is trivial to exploit, and results in high impact to the vulnerable host)

Recommendation

- Ensure the TMUI interface is not accessible to untrusted networks
- F5 recommends upgrading to a fixed software version to fully mitigate this vulnerability
- Implement documented workarounds

Questions?

Contact Michael Gilliam, Manager of Cybersecurity Services, at mgilliam@ddaftech.com or 859.425.7794.