CERT-EU
FOR THE EU INSTITUTIONS, BODIES AND AGENCIES

Security Advisory 2020-031

F5 Critical Vulnerability

July 6, 2020 — v1.1

TLP:WHITE

History:

- *05/07/2020 — v1.0 – Initial publication*
- *06/07/2020 — v1.1 – Update related to existing exploits*

Summary

A new vulnerability has been discovered in the configuration interface of the BIG-IP application delivery controller (ADC) used by some of the world's biggest companies. Attackers can run commands as an unauthorized user and completely compromise a system, including interception of controller application traffic. The vulnerability can be exploited remotely, and is already being actively exploited [1, 4].

Technical Details

Vulnerability, encoded as CVE-2020-5902, received a CVSS score of 10, indicating the highest degree of danger. To exploit it, an attacker needs to send a specifically crafted HTTP request to the server hosting the Traffic Management User Interface (TMUI) utility for BIG-IP configuration. The vulnerability is only exploitable if the management interface is exposed, which generally should not be the case for properly configured systems.

By exploiting this vulnerability, a remote attacker with access to the BIG-IP configuration utility could, without authorization, perform remote code execution. The attacker can create or delete files, disable services, intercept information, run arbitrary system commands and Java code, completely compromise the system, and pursue further targets, such as the internal network.

RCE in this case results from security flaws in multiple components, such as one that allows directory traversal exploitation [2].

Already numerous researchers have started to publicly post exploits for this vulnerability to illustrate how easy it is to exfiltrate data and execute commands on vulnerable devices [4]. **Active exploitation is ongoing**.

Products Affected

The Traffic Management User Interface (TMUI) of the BIG-IP versions [3]:

- 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,
- 11.6.1-11.6.5.1.

Recommendations

F5 Networks has released a patch for this vulnerability. Depending on the version of the software, it should be immediately upgraded to the their respective builds:

- 11.6.5.2,
- 12.1.5.2,
- 13.1.3.4,
- 14.1.2.6,
- 15.1.0.4.

Because there are already many exploits available and **the vulnerability is actively exploited**. CERT-EU highly recommends to patch this products as soon as possible.

Exploitation Detection

To check for exploitation, access logs to the TMUI interface should be investigated for the attempts. In particular, successful requests to `/tmui/login.jsp/..;/*` should be carefully investigated.

Workarounds

In case an immediate update is not possible, other recommendations are given in the F5 BIG-IP bulletin [3].

Also, to mitigate this vulnerability for affected F5 products, the management access to F5 products should only permitted over a secure network.

References

[1] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-5902

[2] https://www.ptsecurity.com/ww-en/about/news/f5-fixes-critical-vulnerability-discovered-by-positive-technologies-in-big-ip-application-delivery-controller/

[3] https://support.f5.com/csp/article/K52145254

[4] https://gist.github.com/ykoster/11148b1783b2205f9a4981b251e522a0