Security Advisory 2022-032

Critical Vulnerability Affecting F5 Devices

May 10, 2022 — v1.1

TLP:WHITE

History:

- *05/05/2022 — v1.0 – Initial publication*
- *10/05/2022 — v1.1 – Updated with information about active exploitation*

Summary

On the 4th or May 2022, F5 released several patches addressing 43 vulnerabilities [1], including one identified as **critical** - CVE-2022-1388 [2]. This vulnerability has the CVSS score of 9.8 out of 10, and it may allow an unauthenticated attacker with network access to the iControl REST interface to execute arbitrary system commands, create or delete files, and disable services [2].

On the 9th of May 2022, Horizon3 - along with other groups - released a proof-of-concept exploit [3]. Moreover, there was an increase of exploitation attempts in the last few days. We advice you to patch as quickly as possible and restrict the access to the F5 BIG-IP management interface only to authorised people.

Technical Details

An attacker with network access to the BIG-IP system through the management port and/or self IP addresses may bypass iControl REST authentication. As stated in the advisory [2], there is no data plane exposure, this vulnerability is a control plane issue only.

Affected Products

- BIG-IP:
  - 16.1.0 - 16.1.2,
  - 15.1.0 - 15.1.5,
  - 14.1.0 - 14.1.4,
  - 13.1.0 - 13.1.4,
  - 12.1.0 - 12.1.6,
  - 11.6.1 - 11.6.5.
- Other F5 products such as BIG-IQ Centralized Management, F5OS-A, F5OS-C, and Traffix SDC are not vulnerable.

To get more detail, please consult the table available on F5 advisory [2].

Recommendations

Apply the patches as soon as possible. CVE-2022-1388 patches have been introduced in versions 17.0.0, 16.1.2.2, 15.1.5.1, 14.1.4.6, and 13.1.5. For the versions 11 and 12 there is no patch available and they will not be fixed.

Update: You may check for any unauthorised actions in at least the following two locations: - /var/log/audit - /var/log/restjavad-audit.0.log

In case of a confirmed compromise, we advise you to rebuild the BIG-IP devices from scratch, and change the internal certificates and passwords.

Workarounds

There are temporary workarounds that can be applied until it is possible to install a fixed version, such as:

- block iControl REST access through the self IP address,
- block iControl REST access through the management interface,
- modify the BIG-IP httpd configuration.

More details can be found in the advisory [2].

References

[1] https://support.f5.com/csp/article/K55879220

[2] https://support.f5.com/csp/article/K23605346

[3] https://github.com/horizon3ai/CVE-2022-1388