Security Advisory 2022-043

Critical Vulnerability in Citrix ADM

June 17, 2022 — v1.0

TLP:WHITE

History:

- *17/06/2022 — v1.0 – Initial publication*

Summary

On the 14th of June 2022, Citrix released security updates to address vulnerabilities in Application Delivery Management that could allow an unauthenticated attacker to log in as administrator [1].

All supported versions of Citrix ADM server and Citrix ADM agent are affected by this vulnerability [2].

Technical Details

The vulnerabilities affects Citrix Application Delivery Management (Citrix ADM), when exploited it could result in the following security issues:

- `CVE-2022-27511` - Corruption of the system by a remote, unauthenticated user. The impact of this can include the reset of the administrator password at the next device reboot, allowing an attacker with ssh access to connect with the default administrator credentials after the device has rebooted.
- `CVE-2022-27512` - Temporary disruption of the ADM license service. The impact of this includes preventing new licenses from being issued or renewed by Citrix ADM.

Affected Products

- Citrix ADM 13.0 before 13.0-85.19
- Citrix ADM 13.1 before 13.1-21.53

Citrix has already updated the ADM cloud service, customers using it do not need to take additional action [1].

Recommendations

CERT-EU recommends to apply the patches provided by Citrix as soon as possible [2]. As a mitigation factor, Citrix recommends that network traffic to the Citrix ADM's IP address is segmented, either physically or logically, from standard network traffic [2].

References

[1] https://www.securityweek.com/attackers-can-exploit-critical-citrix-adm-vulnerability-reset-admin-passwords

[2] https://support.citrix.com/article/CTX460016/citrix-application-delivery-management-security-bulletin-for-cve202227511-and-cve202227512