Severe Vulnerabilities in Citrix Workspace, Virtual Apps and Desktops

February 16, 2023 — v1.0

TLP:CLEAR

History:

- *16/02/2023 — v1.0 – Initial publication*

Summary

On February 14, 2023, Citrix released Security Bulletins regarding severe vulnerabilities affecting its Citrix Workspace, Virtual Apps and Desktops [1]. If exploited, these vulnerabilities could enable attackers to elevate their privileges and take control of the affected system, but they need local access to the target.

It is then highly recommended to install the last security updates.

Technical Details

`CVE-2023-24483` : Improper privilege management flaw leading to privilege escalation to `NT AUTHORITY\SYSTEM` [2].

`CVE-2023-24484` : Improper access control flaw allowing log files to be written to a directory that should be out of reach for regular users [3].

`CVE-2023-24485` : Improper access control flaw leading to privilege escalation [3].

`CVE-2023-24486` : Improper access control flaw leading to session takeover [4].

Affected Products

The following versions are affected by these vulnerabilities:

`CVE-2023-24483` - Citrix Virtual Apps and Desktops before 2212, 2203 LTSR before CU2, and 1912 LTSR before CU6.

`CVE-2023-24484` - Citrix Workspace App for Windows before 2212, 2203 LTSR before CU2, and 1912 LTSR before CU6.

`CVE-2023-24485` - Citrix Workspace App for Windows before 2212, 2203 LTSR before CU2, and 1912 LTSR before CU6.

`CVE-2023-24486` - Citrix Workspace App for Linux before 2302.

Recommendations

CERT-EU highly recommends installing the latest updated versions as soon as possible:

- Citrix Virtual Apps and Desktops 2212 and later versions.
- Citrix Virtual Apps and Desktops 2203 LTSR CU2 and later cumulative updates.
- Citrix Virtual Apps and Desktops 1912 LTSR CU6 and later cumulative updates.
- Citrix Workspace App 2212 and later.
- Citrix Workspace App 2203 LTSR CU2 and later cumulative updates.
- Citrix Workspace App 1912 LTSR CU7 Hotfix 2 (19.12.7002) and later cumulative updates.
- Citrix Workspace app for Linux 2302 and later.

References

[1]   https://www.bleepingcomputer.com/news/security/citrix-fixes-severe-flaws-in-workspace-virtual-apps-and-desktops/

[2]   https://support.citrix.com/article/CTX477616/citrix-virtual-apps-and-desktops-security-bulletin-for-cve202324483

[3]   https://support.citrix.com/article/CTX477617/citrix-workspace-app-for-windows-security-bulletin-for-cve202324484-cve202324485

[4]   https://support.citrix.com/article/CTX477618/citrix-workspace-app-for-linux-security-bulletin-for-cve202324486