CERT-EU
FOR THE EU INSTITUTIONS, BODIES AND AGENCIES

Security Advisory 2020-037

Citrix Workspace Vulnerability

September 23, 2020 — v1.1

TLP:WHITE

History:

- *22/07/2020 — v1.0 – Initial publication*
- *23/09/2020 — v1.1 – Updated with information about new attack vector*

Summary

Citrix Workspace is vulnerable to a remote command execution attack [1]. The flaw sees Workspace app's automatic update feature abused to gain access to a vulnerable Workspace app installation, with the attack vector being a named pipe [3]. Citrix have assigned CVE-2020-8207 to the vulnerability and released updated versions for Workspace app [2].

Since July, there has been found a secondary attack vector, which would allow attackers to elevate privileges and remotely execute arbitrary commands under the SYSTEM account [6, 7].

Technical Details

By sending a crafted message over a named pipe and spoofing the client process ID, the Citrix Workspace Updater Service can be tricked into executing an arbitrary process under the SYSTEM account. Whilst a low privilege account is required to perform the attack, environments that do not implement SMB signing are particularly vulnerable since an attack can be achieved without knowing valid credentials through NTLM credential relaying [1, 3].

A new attack vector has been discovered [7]. The core of the issue lies with a remote command line injection vulnerability that allows attackers to bypass Citrix signed MSI installers using a malicious MSI transform [6, 7].

Products Affected

The issue affects **Citrix Workspace App**.

Recommendations

The issue has been addressed in the following versions of Citrix Workspace app for Windows [1, 7]:

- Citrix Workspace App 2008 or later;
- Citrix Workspace App 1912 LTSR CU1 Hotfix 1 (19.12.1001) and later.

Updates are available [4, 5]. CERT-EU recommends to update the vulnerable application as soon as possible.

References

[1] https://www.pentestpartners.com/security-blog/raining-system-shells-with-citrix-workspace-app/

[2] https://support.citrix.com/article/CTX277662

[3] https://www.theregister.com/2020/07/21/citrix_workspace_app_vuln/

[4] https://www.citrix.com/downloads/workspace-app/windows/

[5] https://www.citrix.com/downloads/workspace-app/workspace-app-for-windows-long-term-service-release/

[6] https://threatpost.com/citrix-workspace-new-attack/159459/

[7] https://www.pentestpartners.com/security-blog/the-return-of-raining-system-shells-with-citrix-workspace-app/