UNISPHERE SOLUTIONS
info@unisphere.co.nz
www.unisphere.co.nz

CYBER GUIDANCE ISSUE 00044

CITRIX WORKSPACE VULNERABILITY REOPENED

DATE ISSUED: 28th September 2020

IMPACT	LOW	MEDIUM	HIGH
EASE OF EXPLOIT	HARD	MEDIUM	EASY

OVERVIEW

Since patching in July, Windows MSI files are still providing an entry point for attackers through a secondary vector, enabling escalation of privileges and Remote Code Execution (RCE). CVE-2020-8207

BREAKDOWN

Using the SYSTEM account, a local user may be allowed to escalate their privileges or remote compromise may occur if the SMB Windows File Sharing is enabled. Previously believed to have been dealt with, according to testers, files with the msi extension for Windows installer packages may convert the pervious bug into vulnerability allowing remote command-line injection. Although the patch now cross references hash values directly from the Citrix repository to reduce the original risk of weak hashes, the oversight of remote connectivity has lead to this further vulnerability being discovered. A common feature used by administrators to push out patches within their Active Directory (AD), the MSI Transform (MST) does not always work unsupervised and users must specify the path to the MST file using their CLI which will merge the MSI file and any changes during installation. Attackers may generate malicious Transforms and replace the original MSI and new MST onto a network share and merely have to wait for a victim to access it.

REMEDIATION STEPS

- Update all Citrix Workspace App for Windows to the latest version
- Monitor networks for unusual activities, sharing and downloads

REFERENCES & RESOURCES

Citrix Advisory: https://support.citrix.com/article/CTX277662
Citrix: https://www.citrix.com/downloads/workspace-app/windows/
Threatpost: https://threatpost.com/citrix-workspace-new-attack/159459/
Security Affairs: https://securityaffairs.co/wordpress/106232/hacking/citrix-workspace-flaw.html