CERT-MU Vulnerability Note

Citrix Windows Virtual Delivery Agent Vulnerability Lets Attackers Escalate to System Privileges

Vulnerability Note: VN-2025-08

Date of Issue: 09 July 2025

Severity Rating: High

Systems Affected:

The vulnerability affects the following supported versions of Windows Virtual Delivery Agent for single-session OS:

Current Release (CR)

- Citrix Virtual Apps and Desktops versions before 2503

Long Term Service Release (LTSR)

- Citrix Virtual Apps and Desktops 2402 LTSR CU2 and earlier versions of 2402 LTSR

Note: Citrix Virtual Apps and Desktops 2203 LTSR is not affected by this vulnerability.

Description

A critical security vulnerability has been discovered in Citrix's Windows Virtual Delivery Agent. This vulnerability could allow attackers with low-level system access to escalate their privileges to SYSTEM level, potentially granting them complete control over affected systems.

Solution

- For Current Release environments, organizations should upgrade to Citrix Virtual Apps and Desktops 2503 or later versions.

- LTSR customers can apply specific updates: 2402 LTSR CU1 Update 1 and 2402 LTSR CU2 Update 1, both available through Citrix support channels.

- For organizations unable to immediately implement patches, Citrix provides a temporary workaround involving a registry modification.

- Administrators can disable the vulnerable component by setting the "Enabled" value to 0 in the HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\CtxExceptionHandler registry key.

More information about the update is available on:
https://support.citrix.com/support-home/kbsearch/article?articleNumber=CTX694820

CVE Information
CVE-2025-6759

Postal address
Mauritian Computer Emergency Response Team (CERT-MU)
Ministry of Information Technology, Communication and Innovation
2nd Floor, Wing A,
Shri Atal Bihari Vajpayee Tower,
Cybercity Ebene,