Hive Pro

Threat Level

Amber

HiveForce Labs

THREAT ADVISORY

VULNERABILITY REPORT

Citrix Resolves Vulnerabilities in Virtual Apps and Workspace Apps

Date of Publication	Admiralty Code	TA Number
February 16, 2023	A1	TA2023084

Summary

First Seen: February 14, 2023
Affected Products: Citrix Virtual Apps, Desktops, and Citrix Workspace App
Impact: Exploiting this vulnerability could allow local attackers to elevate their privileges and gain control over the compromised system.

CVE

CVE	NAME	PATCH
CVE-2023-24483	Privilege Escalation to NT AUTHORITY\SYSTEM	✓
CVE-2023-24484	Improper access control vulnerability in Citrix Workspace App for Windows	✓
CVE-2023-24485	Privilege Escalation in Citrix Workspace app for Windows	✓
CVE-2023-24486	Session Takeover in Citrix Workspace App for Linux	✓

Vulnerability Details

#1

Citrix has addressed security vulnerabilities in its Virtual Apps and Desktops, as well as in its Workspace apps for both Windows and Linux operating systems. These vulnerabilities include CVE-2023-24483, which involves privilege escalation to NT AUTHORITY\SYSTEM on vulnerable Citrix Virtual Apps and Desktops Windows VDA. In addition, Citrix has also resolved two bugs in the Workspace app for Windows, which could potentially be combined to elevate privileges and allow the user to perform actions as a System user.

#2

The first issue, which is identified as CVE-2023-24484, could allow attackers to write log files to directories without proper permissions. The second flaw, CVE-2023-24485, could enable attackers to escalate their privileges. Additionally, a separate vulnerability, tracked as CVE-2023-24486, has been discovered in the Workspace app for Linux, which could allow attackers to take over another user's session.

Vulnerability

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2023-24483	Citrix Virtual Apps and Desktops before 2212, 2203 LTSR before CU2, and 1912 LTSR before CU6.	cpe:2.3:a:citrix:citrix_virtual_apps_windows:*:*:*:*:*:*:*:*	CWE-269
CVE-2023-24484	Citrix Workspace App for Windows before 2212, 2203 LTSR before CU2, and 1912 LTSR before CU6.	cpe:2.3:a:citrix:citrix_virtual_apps_windows:*:*:*:*:*:*:*:*	CWE-284
CVE-2023-24485	Citrix Workspace App for Windows before 2212, 2203 LTSR before CU2, and 1912 LTSR before CU6.	cpe:2.3:a:citrix:citrix_virtual_apps_windows:*:*:*:*:*:*:*:*	CWE-284
CVE-2023-24486	Citrix Workspace App for Linux before 2302.	cpe:2.3:a:citrix:citrix_virtual_apps_linux:*:*:*:*:*:*:*:*	CWE-284

Recommendations

Security Leaders
Asset and vulnerability management solutions should be implemented to ensure that all internet-accessible devices are secure, patched, updated, hardened, and monitored. Integrate and communicate all lessons learned.

Security Engineers

- **Uni5 Users:** This is an actionable threat advisory in HivePro Uni5. Prioritize the vulnerability, identify the impacted assets, and patch them through your Command Center. Test your controls with Uni5's Breach & Attack Simulation.

- **All Engineers:** Refer to and action upon the 'Potential MITRE ATT&CK TTPs' & 'Patch Details' on the following pages.

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	**TA0001** Initial Access	**TA0002** Execution	**TA0003** Persistence
TA0008 Lateral Movement	**T1588** Obtain Capabilities	**T1588.006** Vulnerabilities	**T1543** Create or Modify System Process
T1210 Exploitation of Remote Services	**T1190** Exploit Public-Facing Application	**T1078** Valid Accounts	**T1098** Account Manipulation

Patch Links

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

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

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

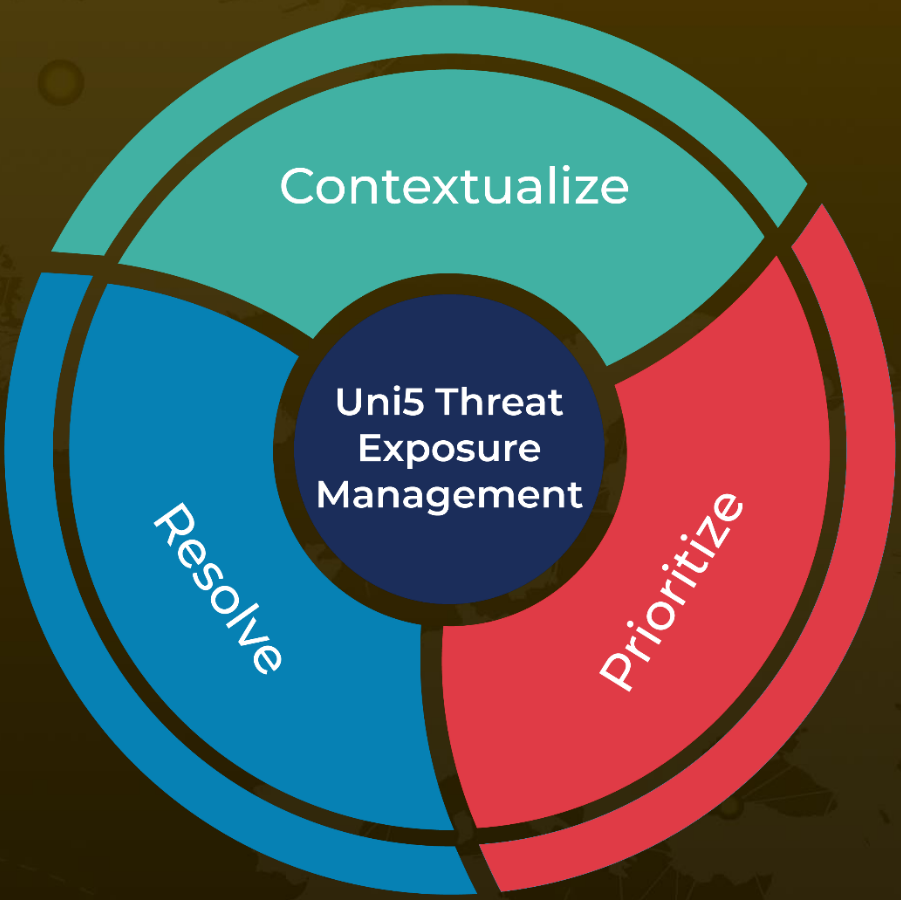
References

https://support.citrix.com/knowledge-center/search/#/All%20Products?ct=Security%20Bulletins&searchText=&sortBy=Created%20date&pageIndex=1

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

February 16, 2023 • 1:11 AM

More at www.hivepro.com