Advisory Alert

Alert Number: AAA20250618 **Date:** June 18, 2025

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Veeam	**Critical**	Remote Code Execution Vulnerability
Citrix	**Critical**	Memory Overread Vulnerability
SUSE	**High**	Multiple Linux Kernel Vulnerabilities
Citrix	**High**	Input Validation Vulnerability
Apache Tomcat	**High**	Multiple Vulnerabilities
Veeam	**High**, **Medium**	Multiple Vulnerabilities

Description

Affected Product	**Veeam**
Severity	**Critical**
Affected Vulnerability	Remote Code Execution Vulnerability (CVE-2025-23121)
Description	Veeam has released security updates addressing a remote code execution vulnerability that exists in their products. **CVE-2025-23121** - A vulnerability allowing remote code execution (RCE) on the Backup Server by an authenticated domain user. Veeam advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Veeam Backup & Replication Versions - 12.3.1.1139 and all Versions Prior to 12 builds.
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.veeam.com/kb4743

Affected Product	**Citrix**
Severity	**Critical**
Affected Vulnerability	Input Validation Vulnerability (CVE-2025-5777)
Description	Citrix has released security updates addressing an input validation vulnerability that exists in their products. **CVE-2025-5777** - An insufficient input validation vulnerability in NetScaler can lead to an out-of-bounds memory read when it is configured as a Gateway (VPN virtual server, ICA Proxy, CVPN, or RDP Proxy) or as an AAA virtual server. Citrix advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	NetScaler ADC and NetScaler Gateway 14.1 BEFORE 14.1-43.56 NetScaler ADC and NetScaler Gateway 13.1 BEFORE 13.1-58.32 NetScaler ADC 13.1-FIPS and NDcPP BEFORE 13.1-37.235-FIPS and NDcPP NetScaler ADC 12.1-FIPS BEFORE 12.1-55.328-FIPS
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.citrix.com/support-home/kbsearch/article?articleNumber=CTX693420&articleURL=NetScaler_ADC_and_NetScaler_Gateway_Security_Bulletin_for_CVE_2025_5349_and_CVE_2025_5777

Affected Product	**SUSE**
Severity	**High**
Affected Vulnerability	Multiple Linux Kernel Vulnerabilities
Description	SUSE has released security updates addressing multiple linux kernel vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to cause integer overflow, null pointer dereference, memory leak. SUSE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	OpenSUSE Leap 15.3 SUSE Enterprise Storage 7.1 SUSE Linux Enterprise High Availability Extension 15 SP3 SUSE Linux Enterprise High Performance Computing 12 SP5, 15 SP3, LTSS 15 SP3 SUSE Linux Enterprise Live Patching 12-SP5, 15-SP3, 15-SP7 SUSE Linux Enterprise Micro 5.1, 5.2 SUSE Linux Enterprise Micro for Rancher 5.2 SUSE Linux Enterprise Real Time 15 SP7 SUSE Linux Enterprise Server 12 SP5, 12 SP5 LTSS, Server 12 SP5 LTSS Extended Security SUSE Linux Enterprise Server 15 SP3, 15 SP3 Business Critical Linux, 15 SP3 LTSS, 15 SP7 SUSE Linux Enterprise Server for SAP Applications 12 SP5, 15 SP3, 15 SP7 SUSE Manager Proxy 4.2 SUSE Manager Retail Branch Server 4.2 SUSE Manager Server 4.2 SUSE Real Time Module 15-SP7
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.suse.com/support/update/announcement/2025/suse-su-202501972-1/ • https://www.suse.com/support/update/announcement/2025/suse-su-202501982-1/ • https://www.suse.com/support/update/announcement/2025/suse-su-202501983-1/

Affected Product	**Citrix**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-5349, CVE-2025-4879, CVE-2025-0320)
Description	Citrix has released security updates addressing multiple vulnerabilities that exist in their products. **CVE-2025-5349** - Incorrect access control in the NetScaler Management Interface allows an attacker with access to NSIP, Cluster Management IP, or a local GSLB Site IP to gain unauthorized interface access **CVE-2025-4879** - A local privilege escalation vulnerability in Citrix Workspace app for Windows allows an attacker with local access to elevate from a low-privilege account to SYSTEM level. It exploits how the Workspace app interacts with the App Protection service. **CVE-2025-0320** - A local privilege escalation vulnerability allows an unprivileged local user to elevate privileges to SYSTEM on Windows machines where the Secure Access Client is installed. Citrix advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	NetScaler ADC and NetScaler Gateway 14.1 BEFORE 14.1-43.56 NetScaler ADC and NetScaler Gateway 13.1 BEFORE 13.1-58.32 NetScaler ADC 13.1-FIPS and NDcPP BEFORE 13.1-37.235-FIPS and NDcPP NetScaler ADC 12.1-FIPS BEFORE 12.1-55.328-FIPS Citrix Secure Access Client for Windows versions BEFORE 25.5.1.15 Citrix Workspace app for Windows versions before 2409 (Current Release (CR)) Citrix Workspace app for Windows versions before 2402 LTSR CU2 Hotfix 1 Citrix Workspace app for Windows versions before 2402 LTSR CU3 Hotfix 1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://support.citrix.com/support-home/kbsearch/article?articleNumber=CTX693420&articleURL=NetScaler_ADC_and_NetScaler_Gateway_Security_Bulletin_for_CVE_2025_5349_and_CVE_2025_5777 • https://support.citrix.com/support-home/kbsearch/article?articleNumber=CTX694718&articleURL=Citrix_Workspace_app_for_Windows_Security_Bulletin_CVE_2025_4879 • https://support.citrix.com/support-home/kbsearch/article?articleNumber=CTX694724&articleURL=Citrix_Secure_Access_Client_for_Windows_Security_Bulletin_for_CVE_2025_0320

Affected Product	**Apache Tomcat**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-49125, CVE-2025-49124, CVE-2025-48988, CVE-2025-48976)
Description	Apache Tomcat has released security updates addressing Multiple Vulnerabilities that exists in their products. These vulnerabilities could be exploited by malicious users to cause authentication bypass, Windows untrusted search path (side-loading) and Denial-of-Service. Apache Tomcat advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Apache Tomcat Versions • 11.0.0-M1 through 11.0.7 • 10.1.0-M1 through 10.1.41 • 9.0.0.M1 through 9.0.105
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://tomcat.apache.org/security-9.html#Fixed_in_Apache_Tomcat_9.0.106 • https://tomcat.apache.org/security-10.html#Fixed_in_Apache_Tomcat_10.1.42 • https://tomcat.apache.org/security-11.html#Fixed_in_Apache_Tomcat_11.0.8

Affected Product	**Veeam**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-24286, CVE-2025-24287)
Description	Veeam has released security updates addressing Multiple Vulnerabilities that exist in their products. **CVE-2025-24286** - A vulnerability allowing an authenticated user with the Backup Operator role to modify backup jobs, which could execute arbitrary code. **CVE-2025-24287** - A vulnerability allowing local system users to modify directory contents, allowing for arbitrary code execution on the local system with elevated permissions. Veeam advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Veeam Backup & Replication 12.3.1.1139 and all Versions Prior to 12 builds. Veeam Agent for Microsoft Windows 6.3.1.1074 and all Versions Prior to 6 builds.
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.veeam.com/kb4743

Disclaimer

The information provided are gathered from official service provider's websites and portals. FinCSIRT strongly recommends members to apply security fixes as per the given guidelines, following the organization's patch and change management procedures to protect systems from potential threats.