CYBER ADVISORY

TLP:CLEAR
8 April 2025

Dell Unity, UnityVSA, Unity XT - Multiple Vulnerabilities

Dell Unity | Remote Code Execution | Full System Takeover | Upgrade Available

The California Cybersecurity Integration Center (Cal-CSIC) has become aware of multiple critical and high vulnerabilities in the Dell Unity product line, including Dell Unity, UnityVSA, and Unity XT. The most serious vulnerability disclosed could allow an unauthenticated attacker to remotely access and conduct arbitrary command execution as root (CVE-2025-22398).[1] There are sixteen (16) total vulnerabilities associated with the Dell Unity products affecting all versions prior to 5.4. Dell has provided an upgrade to remediate the affected products and recommends updating to Dell Unity OE Version 5.5.0.0.5.259 or higher as soon as practicable. [2] No proof of concept has been posted publicly and there is currently no known exploitation in the wild. [3]

Title	CVE (CVSS Score)	Description	Affected Versions
Dell Unity	CVE-2025-22398 (**9.8**)	Dell Unity, version(s) 5.4 and prior, contain(s) an Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') vulnerability. An unauthenticated attacker with remote access could potentially exploit this vulnerability, leading to arbitrary command execution as root. Exploitation may lead to a system take over by an attacker. This vulnerability is considered critical as it can be leveraged to completely compromise the operating system.	Version 5.4 and prior

WARNING: This document is the exclusive property of the California Cybersecurity Integration Center (CAL-CSIC) and abides by Traffic Light Protocol (TLP) standards for distribution purposes. It may contain information exempt from public release under the California Public Records Act (Govt. Code Sec. 6250, et seq.). Recipients must control, store, handle, transmit, distribute, and dispose of this product in accordance with the TLP standard relating to shared intelligence. Do not release to the public, media, or other personnel who do not have a valid need-to-know without prior approval of an authorized CAL-CSIC official.

Dell Unity	CVE-2025-24383 (**9.1**)	Dell Unity, version(s) 5.4 and prior, contain(s) an Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') vulnerability. An unauthenticated attacker with remote access could potentially exploit this vulnerability to delete arbitrary files. This vulnerability is considered critical as it can be leveraged to delete critical system files as root.	Version 5.4 and prior
Dell Unity	CVE-2025-24381 (**8.8**)	Dell Unity, version(s) 5.4 and prior, contain(s) an URL Redirection to Untrusted Site ('Open Redirect') vulnerability. An unauthenticated attacker with remote access could potentially exploit this vulnerability, leading to a targeted application user being redirected to arbitrary web URLs. The vulnerability could be leveraged by attackers to conduct phishing attacks that cause users to divulge sensitive information. Exploitation may allow for session theft.	Version 5.4 and prior
Dell Unity	CVE-2025-49563 (**7.8**)	Dell Unity, version(s) 5.4 and prior, contain(s) an Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') vulnerability. A low privileged attacker with local access could potentially exploit this vulnerability, leading to execution of arbitrary operating system commands with root privileges and elevation of privileges.	Version 5.4 and prior

WARNING: This document is the exclusive property of the California Cybersecurity Integration Center (CAL-CSIC) and abides by Traffic Light Protocol (TLP) standards for distribution purposes. It may contain information exempt from public release under the California Public Records Act (Govt. Code Sec. 6250, et seq.). Recipients must control, store, handle, transmit, distribute, and dispose of this product in accordance with the TLP standard relating to shared intelligence. Do not release to the public, media, or other personnel who do not have a valid need-to-know without prior approval of an authorized CAL-CSIC official.

Dell Unity	CVE-2025-49564 (**7.8**)	Dell Unity, version(s) 5.4 and prior, contain(s) an Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') vulnerability. A low privileged attacker with local access could potentially exploit this vulnerability, leading to execution of arbitrary operating system commands with root privileges and elevation of privileges.	Version 5.4 and prior

The Cal-CSIC recommends immediately upgrading Dell Unity to Dell Unity OE Version 5.5.0.0.5.259 or higher.

For more information on the additional vulnerabilities not listed above and applying the security update, please refer to the Dell Technologies Security Update.

Organization, Source, Reference, and Dissemination Information

Organization Description	California Government Code § 8586.5 established the California Cybersecurity Integration Center (Cal-CSIC) as the central organizing hub of state government's cybersecurity activities, including information sharing, intelligence analysis, incident response, and overarching cybersecurity strategy. The Cal-CSIC is responsible for reducing the likelihood and severity of cyber incidents that could damage California's economy, critical infrastructure, and public or private sector networks in our state.
Customer Feedback	If you need further information about this issue, contact the Cal-CSIC at our email address CalCSIC@caloes.ca.gov or by telephone at (833) REPORT1.
Source Summary Statement	This report was compiled from a variety of sources, predominately open-source reporting.
Handling Caveats	**Traffic Light Protocol (TLP):** Recipients may share TLP:CLEAR information with the world; there is no limit on disclosure. Subject to standard copyright rules, TLP:CLEAR information may be shared without restriction.

WARNING: This document is the exclusive property of the California Cybersecurity Integration Center (CAL-CSIC) and abides by Traffic Light Protocol (TLP) standards for distribution purposes. It may contain information exempt from public release under the California Public Records Act (Govt. Code Sec. 6250, et seq.). Recipients must control, store, handle, transmit, distribute, and dispose of this product in accordance with the TLP standard relating to shared intelligence. Do not release to the public, media, or other personnel who do not have a valid need-to-know without prior approval of an authorized CAL-CSIC official.

[1] Cyber Security News; "Multiple Dell Unity Vulnerabilities Let Attackers Compromise Affected System"; https://cybersecuritynews.com/multiple-dell-unity-vulnerabilities/; accessed 7 April 2025.
[2] Red-Team News; "Critical OS Command Injection Vulnerability in Dell Unity (CVE-2025-24383) Poses Severe Risk"; https://redteamnews.com/red-team/cve/critical-os-command-injection-vulnerability-in-dell-unity-cve-2025-24383-poses-severe-risk/; accessed 7 April 2025.
[3] Github.com; "CVE-2025-24383; https://github.com/advisories/ghsa-jfxx-2225-hwx8; accessed 7 April 2025.

WARNING: This document is the exclusive property of the California Cybersecurity Integration Center (CAL-CSIC) and abides by Traffic Light Protocol (TLP) standards for distribution purposes. It may contain information exempt from public release under the California Public Records Act (Govt. Code Sec. 6250, et seq.). Recipients must control, store, handle, transmit, distribute, and dispose of this product in accordance with the TLP standard relating to shared intelligence. Do not release to the public, media, or other personnel who do not have a valid need-to-know without prior approval of an authorized CAL-CSIC official.