Advisory Alert

Alert Number: AAA20250925 **Date:** September 25, 2025

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
SolarWinds	**Critical**	Unauthenticated AjaxProxy Deserialization Remote Code Execution Vulnerability
SUSE	**High**	Multiple Vulnerabilities
Cisco	**High**, Medium	Multiple Vulnerabilities
Red Hat	**High**, Medium	Multiple Vulnerabilities
Ubuntu	**High**, Medium	Multiple Vulnerabilities
Drupal	**High**, Medium, Low	Multiple Vulnerabilities

Description

Affected Product	**SolarWinds**
Severity	**Critical**
Affected Vulnerability	Unauthenticated Ajaxproxy Deserialization Remote Code Execution Vulnerability (CVE-2025-26399)
Description	SolarWinds has released security updates an Unauthenticated AjaxProxy Deserialization Remote Code Execution Vulnerability that exists in SolarWinds Web Help Desk. **CVE-2025-26399** - SolarWinds Web Help Desk was found to be susceptible to an unauthenticated AjaxProxy deserialization remote code execution vulnerability that, if exploited, would allow an attacker to run commands on the host machine. SolarWinds advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	SolarWinds Web Help Desk 12.8.7 and all previous versions
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.solarwinds.com/trust-center/security-advisories/cve-2025-26399

Affected Product	**SUSE**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities
Description	SUSE has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to compromise the affected system. SUSE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	openSUSE Leap 15.5 SUSE Linux Enterprise High Performance Computing 12 SP5, 15 SP5 SUSE Linux Enterprise High Performance Computing ESPOS 15 SP5 SUSE Linux Enterprise High Performance Computing LTSS 15 SP5 SUSE Linux Enterprise Live Patching 12-SP5, 15-SP5, 15-SP6 SUSE Linux Enterprise Micro 5.5 SUSE Linux Enterprise Real Time 15 SP5, 15 SP6 SUSE Linux Enterprise Server 12 SP5, 15 SP5 SUSE Linux Enterprise Server 15 SP5 LTSS SUSE Linux Enterprise Server 15 SP6 SUSE Linux Enterprise Server for SAP Applications 12 SP5, 15 SP5, 15 SP6
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.suse.com/support/update/announcement/2025/suse-su-202503350-1/ • https://www.suse.com/support/update/announcement/2025/suse-su-202503342-1/ • https://www.suse.com/support/update/announcement/2025/suse-su-202503344-1/ • https://www.suse.com/support/update/announcement/2025/suse-su-202503343-1/ • https://www.suse.com/support/update/announcement/2025/suse-su-202503341-1/ • https://www.suse.com/support/update/announcement/2025/suse-su-202503339-1/ • https://www.suse.com/support/update/announcement/2025/suse-su-202503336-1/ • https://www.suse.com/support/update/announcement/2025/suse-su-202503337-1/

Affected Product	**Cisco**
Severity	**High**, Medium
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-20312, CVE-2025-20352, CVE-2025-20313, CVE-2025-20314, CVE-2025-20315, CVE-2025-20334, CVE-2025-20160, CVE-2025-20327, CVE-2025-20311, CVE-2025-20240, CVE-2025-20338, CVE-2025-20149, CVE-2025-20339, CVE-2025-20316, CVE-2025-20365, CVE-2025-20364, CVE-2025-20293)
Description	Cisco has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to cause Denial of Service, Remote Code Execution, Authentication Bypass, Command Injection, Cross-Site Scripting. Cisco advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Multiple Products
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://sec.cloudapps.cisco.com/security/center/publicationListing.x

Affected Product	**Red Hat**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities
Description	Red Hat has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to compromise the affected system. Red Hat advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	JBoss Enterprise Application Platform 7.1 EUS 7.1 x86_64 JBoss Enterprise Application Platform 7.3 EUS 7.3 x86_64 Red Hat CodeReady Linux Builder for ARM 64 - Extended Update Support 9.4 aarch64 Red Hat CodeReady Linux Builder for IBM z Systems - Extended Update Support 9.4 s390x Red Hat CodeReady Linux Builder for Power, little endian - Extended Update Support 9.4 ppc64le Red Hat CodeReady Linux Builder for x86_64 - Extended Update Support 9.4 x86_64 Red Hat Enterprise Linux for ARM 64 - 4 years of updates 9.4 aarch64 Red Hat Enterprise Linux for ARM 64 - Extended Update Support 9.4 aarch64 Red Hat Enterprise Linux for IBM z Systems - 4 years of updates 9.4 s390x Red Hat Enterprise Linux for IBM z Systems - Extended Update Support 9.4 s390x Red Hat Enterprise Linux for Power, little endian - Extended Update Support 9.4 ppc64le Red Hat Enterprise Linux for Power, little endian 8 ppc64le Red Hat Enterprise Linux for x86_64 - Extended Update Support 9.4 x86_64 Red Hat Enterprise Linux for x86_64 - Extended Update Support Extension 8.6 x86_64 Red Hat Enterprise Linux for x86_64 - Extended Update Support Extension 8.8 x86_64 Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 8.6 x86_64 Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 8.8 x86_64 Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 9.4 x86_64 Red Hat Enterprise Linux for x86_64 8 x86_64 Red Hat Enterprise Linux Server - AUS 9.4 x86_64 Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 8.6 ppc64le Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 8.8 ppc64le Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 9.4 ppc64le
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://access.redhat.com/errata/RHSA-2025:16669 • https://access.redhat.com/errata/RHSA-2025:16668 • https://access.redhat.com/errata/RHSA-2025:16667 • https://access.redhat.com/errata/RHSA-2025:16583 • https://access.redhat.com/errata/RHSA-2025:16582 • https://access.redhat.com/errata/RHSA-2025:16580

Affected Product	**Ubuntu**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities
Description	Ubuntu has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to compromise the affected system. Ubuntu advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Ubuntu 25.04 Ubuntu 24.04 Ubuntu 22.04
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://ubuntu.com/security/notices/USN-7769-1 • https://ubuntu.com/security/notices/USN-7764-1

Affected Product	**Drupal**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-10929, CVE-2025-10928, CVE-2025-10926)
Description	Drupal has released security updates addressing multiple vulnerabilities that exist in their products. **CVE-2025-10929** - This vulnerability allows an attacker to spoof a request IP address (as Drupal sees it), potentially bypassing a variety of controls. **CVE-2025-10928** - This module enables users to sign in with an access code instead of entering user names and passwords. When users are allowed to pick their own access codes, they can guess other users' access codes based on the fact that access codes need to be unique and the system warns if the code of their choice is taken. **CVE-2025-10926** - The module doesn't sufficiently filter data using some of the included field formatters leading to a Cross-site Scripting (XSS) vulnerability. Drupal advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Reverse Proxy Header module versions prior to 1.1.2 Access code module versions prior to 2.0.5 JSON Field module versions prior to 1.5
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.drupal.org/sa-contrib-2025-111 • https://www.drupal.org/sa-contrib-2025-108 • https://www.drupal.org/sa-contrib-2025-106

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.