Advisory Alert

Alert Number: AAA20240612 **Date:** June 12, 2024

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
HPE	**Critical**	Multiple Vulnerabilities
Microsoft	**Critical**	Multiple Vulnerabilities
Dell	**High**	Multiple Vulnerabilities
Red Hat	**High**, **Medium**	Multiple Vulnerabilities
HPE	**High**, **Medium**	Multiple Vulnerabilities
SAP	**High**, **Medium**, **Low**	Multiple Vulnerabilities
Ubuntu	**High**, **Medium**, **Low**	Multiple Vulnerabilities

Description

Affected Product	**HPE**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-45229, CVE-2023-45230, CVE-2023-45231, CVE-2023-45232, CVE-2023-45233, CVE-2023-45234, CVE-2023-45235, CVE-2023-45236, CVE-2023-45237, CVE-2021-38575, CVE-2021-38578, CVE-2005-4837, CVE-2021-33813, CVE-2021-42392, CVE-2020-11022, CVE-2020-11023, CVE-2017-15806, CVE-2020-7692, CVE-2021-22573, CVE-2020-11988, CVE-2004-2300, CVE-2002-1570, CVE-2022-1471, CVE-2022-45868, CVE-2022-40150, CVE-2023-34453, CVE-2022-41404, CVE-2023-34455, CVE-2023-1436, CVE-2023-34454, CVE-2022-45685, CVE-2022-40149, CVE-2017-9096, CVE-2022-23221, CVE-2022-45693, CVE-2022-24839)
Description	HPE has released security updates addressing multiple vulnerabilities that exist in their products. Exploitation of these vulnerabilities may lead to Arbitrary Code Execution, Denial of Service (DoS), Buffer Overflow, Remote Code Execution. HPE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	HPE ProLiant DL360 Gen10 Plus server - Prior to v2.00_03-06-2024 HPE ProLiant DL380 Gen10 Plus server - Prior to v2.00_03-06-2024 HPE ProLiant ML30 Gen10 Plus server - Prior to v2.10_05-16-2024 HPE ProLiant MicroServer Gen10 Plus - Prior to v3.10_05-16-2024 HPE ProLiant MicroServer Gen10 Plus v2 - Prior to v2.10_05-16-2024 HPE ProLiant DL20 Gen10 Server - Prior to v3.10_03-21-2024 HPE ProLiant DL160 Gen10 Server - Prior to v3.10_02-22-2024 HPE ProLiant DL180 Gen10 Server - Prior to v3.10_02-22-2024 HPE ProLiant DL360 Gen10 Server - Prior to v3.10_02-22-2024 HPE ProLiant DL380 Gen10 Server - Prior to v3.10_02-22-2024 HPE ProLiant DL560 Gen10 Server - Prior to v3.10_02-22-2024 HPE ProLiant ML30 Gen10 Server - Prior to v3.10_05-16-2024 HPE ProLiant ML110 Gen10 Server - Prior to v3.10_02-22-2024 HPE ProLiant ML350 Gen10 Server - Prior to v3.10_02-22-2024 HPE ProLiant DL20 Gen9 Server - Prior to v3.40_03-21-2024 HPE ProLiant ML30 Gen9 Server - Prior to v3.40_03-21-2024 HPE Synergy 480 Gen11 Compute Module - Prior to v2.16_03-01-2024 HPE Synergy 480 Gen10 Plus Compute Module - Prior to v2.00_02-22-2024 HPE ProLiant BL460c Gen10 Server Blade - Prior to v3.10_02-22-2024 HPE Synergy 480 Gen10 Compute Module - Prior to v3.10_02-22-2024 HPE Synergy 660 Gen10 Compute Module - Prior to v3.10_02-22-2024 HPE Apollo 4200 Gen10 Plus System - Prior to v2.00_02-22-2024 HPE ProLiant XL220n Gen10 Plus Server - Prior to v2.00_02-22-2024 HPE ProLiant XL290n Gen10 Plus Server - Prior to v2.00_02-22-2024 HPE Apollo 2000 Gen10 Plus System - Prior to v2.00_02-22-2024 HPE ProLiant XL170r Gen10 Server - Prior to v3.10_02-22-2024 HPE ProLiant XL190r Gen10 Server - Prior to v3.10_02-22-2024 HPE Apollo 2000 System - Prior to v3.10_02-22-2024 HPE ProLiant e910 Server Blade - Prior to v3.10_02-22-2024 HPE ProLiant e910t Server Blade - Prior to v3.10_02-22-2024 HPE Edgeline e920 Server Blade - Prior to v2.00_02-22-2024 HPE Edgeline e920d Server Blade - Prior to v2.00_02-22-2024 HPE Edgeline e920t Server Blade - Prior to v2.00_02-22-2024 HPE Compute Edge Server e930t - Prior to v2.16_03-01-2024 HPE ProLiant RL300 Gen11 - Prior to v1.60_03-07-2024 HPE ProLiant DX170r Gen10 server - Prior to v3.10_02-22-2024 HPE ProLiant DX190r Gen10 server - Prior to v3.10_02-22-2024 HPE ProLiant DX360 Gen10 Plus server - Prior to v2.00_03-06-2024 HPE ProLiant DX380 Gen10 Plus server - Prior to v2.00_03-06-2024 HPE ProLiant DX220n Gen10 Plus server - Prior to v2.00_02-22-2024 HPE ProLiant DX360 Gen10 server - Prior to v3.10_02-22-2024 HPE ProLiant DX380 Gen10 server - Prior to v3.10_02-22-2024 HPE ProLiant DX560 Gen10 server - Prior to v3.10_02-22-2024 HPE ProLiant DX4200 Gen10 server - Prior to v2.00_02-22-2024 HPE Unified Topology Manager (UTM) - Prior to v4.4
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbhf04593en_us&docLocale=en_US • https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbgn04655en_us&docLocale=en_US

Affected Product	**Microsoft**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-35248, CVE-2024-30104, CVE-2024-30103, CVE-2024-30102, CVE-2024-30101, CVE-2024-30100, CVE-2024-30099, CVE-2024-30097, CVE-2024-30096, CVE-2024-30052, CVE-2024-37325, CVE-2024-35265, CVE-2024-35263, CVE-2024-35254, CVE-2024-35253, CVE-2024-35252, CVE-2024-35249, CVE-2024-30095, CVE-2024-30094, CVE-2024-30093, CVE-2024-30091, CVE-2024-30090, CVE-2024-30089, CVE-2024-30088, CVE-2024-30087, CVE-2024-30086, CVE-2024-30085, CVE-2024-30084, CVE-2024-30083, CVE-2024-30068, CVE-2024-30067, CVE-2024-30066, CVE-2024-30065, CVE-2024-30064, CVE-2024-30063, CVE-2024-30062, CVE-2024-29060, CVE-2024-29187, CVE-2023-50868, CVE-2024-35255, CVE-2024-35250, CVE-2024-30082, CVE-2024-30080, CVE-2024-30078, CVE-2024-30077, CVE-2024-30076, CVE-2024-30075, CVE-2024-30074, CVE-2024-30072, CVE-2024-30070, CVE-2024-30069)
Description	Microsoft has released critical security updates for June 2024. This release includes fixes for several vulnerabilities across various Microsoft products. It is highly recommended that you apply these security patches immediately to protect systems from potential threats.
Affected Products	Microsoft Dynamics 365 Business Central 2023 Release Wave 1 Application Build 22.13.64344, Platform Build 22.0 Microsoft Office 2016 (64-bit edition) 16.0.5452.1000 Microsoft Office 2016 (32-bit edition) 16.0.5452.1000 Microsoft Office LTSC 2021 for 32-bit editions and 64-bit editions Microsoft 365 Apps for Enterprise for 32-bit editions and 64-bit editions Microsoft Office 2019 for 32-bit editions and 64-bit editions Microsoft Outlook 2016 (64-bit edition and 32-bit edition) 16.0.5452.1000 Microsoft SharePoint Server Subscription Edition 16.0.17328.20362 Microsoft SharePoint Server 2019 16.0.10411.20004 Microsoft SharePoint Enterprise Server 2016 16.0.5452.1000 Windows Server 2016 (Server Core installation) 10.0.14393.7070 Windows Server 2016 10.0.14393.7070 Windows 10 Version 1607 for x64-based Systems and 32-bit Systems 10.0.14393.7070 Windows 10 for x64-based Systems and 32-bit Systems 10.0.10240.20680 Windows Server 2022, 23H2 Edition (Server Core installation) 10.0.25398.950 Windows 11 Version 23H2 for x64-based Systems 10.0.22631.3737 Windows 11 Version 23H2 for ARM64-based Systems 10.0.22631.3737 Windows 10 Version 22H2 for 32-bit Systems 10.0.19043.4529 Windows 10 Version 22H2 for ARM64-based Systems 10.0.19043.4529 Windows 10 Version 22H2 for x64-based Systems 10.0.19043.4529 Windows 11 Version 22H2 for x64-based Systems 10.0.22621.3737 Windows 11 Version 22H2 for ARM64-based Systems 10.0.22621.3737 Windows 10 Version 21H2 for x64-based Systems 10.0.19043.4529 Windows 10 Version 21H2 for ARM64-based Systems 10.0.19043.4529 Windows 10 Version 21H2 for 32-bit Systems 10.0.19043.4529 Windows 11 version 21H2 for ARM64-based Systems Windows 11 version 21H2 for x64-based Systems 10.0.22000.3019 Windows Server 2022 (Server Core installation) 10.0.20348.2527 Windows Server 2022 (Server Core installation) 10.0.20348.2522 Windows Server 2022 10.0.20348.2527 Windows Server 2022 10.0.20348.2522 Windows Server 2019 (Server Core installation) 10.0.17763.5936 Windows Server 2019 10.0.17763.5936 Windows 10 Version 1809 for ARM64-based Systems 10.0.17763.5936 Windows 10 Version 1809 for x64-based Systems 10.0.17763.5936 Windows 10 Version 1809 for 32-bit Systems 10.0.17763.5936 Microsoft Visual Studio 2022 version 17.10 (17.10.2), 17.8 (17.8.11), 17.6 (17.6.16), 17.4 (17.4.20) Microsoft Visual Studio 2019 version 16.11 (includes 16.0 - 16.10) 16.11.37 Microsoft Visual Studio 2017 version 15.9 (includes 15.0 - 15.8) 15.9.63 Azure Data Science Virtual Machines for Linux 24.05.24 Microsoft Dynamics 365 (on-premises) version 9.1 1.29 Azure Monitor Agent 1.26.0 Azure File Sync v17.0 (17.3), v18.0 (18.1), v16.0 (17.3) Azure Storage Movement Client Library for .NET 2.0.5 Microsoft Dynamics 365 Business Central 2023 Release Wave 2 Application Build 23.7.18957, Platform Build 23.0. Microsoft Dynamics 365 Business Central 2024 Release Wave 1 Application Build 24.1.19498, Platform Build 24.0. Windows Server 2012 R2 (Server Core installation) 6.3.9600.22023 Windows Server 2012 R2 6.3.9600.22023 Windows Server 2012 (Server Core installation) 6.2.9200.24919 Windows Server 2012 6.2.9200.24919 Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation) 6.1.7601.27170 Windows Server 2008 R2 for x64-based Systems Service Pack 1 6.1.7601.27170 Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation) 6.0.6003.22720 Windows Server 2008 for x64-based Systems Service Pack 2 6.0.6003.22720 Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation) 6.0.6003.22720 Windows Server 2008 for 32-bit Systems Service Pack 2 6.0.6003.22720 Azure Identity Library for Python 1.16.1 Azure Identity Library for C++ 1.7.0 Azure Identity Library for JavaScript 4.2.1 Azure Identity Library for Java 1.12.2 Microsoft Authentication Library (MSAL) for Node.js 2.9.2 Microsoft Authentication Library (MSAL) for .NET 4.61.3 Azure Identity Library for Go 1.6.0 Microsoft Authentication Library (MSAL) for Java 1.15.1 Azure Identity Library for .NET 1.11.4
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://msrc.microsoft.com/update-guide/releaseNote/2024-Jun

Affected Product	**Dell**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2021-33200, CVE-2022-20154, CVE-2023-46589, CVE-2023-35116, CVE-2023-7104, CVE-2024-25062, CVE-2023-29469, CVE-2023-28484, CVE-2023-45322, CVE-2022-23829)
Description	Dell has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to compromise the affected systems. Dell advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	NetWorker vProxy OVA • Versions 19.10 through 19.10.0.2 • Versions 19.9 through 19.9.0.6 • Versions 19.8 through 19.8.0.4 • Versions prior to 19.8 NetWorker Authentication Service, NetWorker Server • Versions 19.10 through 19.10.0.2 • Versions 19.9 through 19.9.0.6 • Versions 19.8 through 19.8.0.4 • Versions prior to 19.8 NetWorker Authentication Service, NetWorker WebUI • Versions 19.10 through 19.10.0.2 • Versions 19.9 through 19.9.0.6 • Versions 19.8 through 19.8.0.4 • Versions prior to 19.8 NetWorker Server • Versions 19.10 through 19.10.0.2 • Versions 19.9 through 19.9.0.6 • Versions 19.8 through 19.8.0.4 • Versions prior to 19.8 PowerEdge R6415 BIOS - Versions prior to 1.17.0 PowerEdge R7415 BIOS - Versions prior to 1.17.0 PowerEdge R7425 BIOS - Versions prior to 1.17.0 PowerEdge XE8545 BIOS - Versions prior to 2.3.6 PowerEdge C6525 BIOS - Versions prior to 2.3.6 PowerEdge R6515 BIOS - Versions prior to 2.3.6 PowerEdge R7515 BIOS - Versions prior to 2.3.6 PowerEdge R6525 BIOS - Versions prior to 2.3.6 PowerEdge R7525 BIOS - Versions prior to 2.3.6 Dell EMC XC Core XC7525 BIOS - Versions prior to 2.3.6
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.dell.com/support/kbdoc/en-us/000225942/dsa-2024-269-security-update-for-dell-networker-vproxy-linux-kernel-vulnerabilities • https://www.dell.com/support/kbdoc/en-us/000225945/dsa-2024-248-security-update-for-dell-networker-multiple-component-vulnerabilities • https://www.dell.com/support/kbdoc/en-us/000225975/dsa-2024-149-dell-poweredge-server-security-update-for-amd-server-vulnerabilities

Affected Product	**Red Hat**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2021-47013, CVE-2023-1118, CVE-2023-1998, CVE-2023-4155, CVE-2023-5072, CVE-2023-5090, CVE-2023-51779, CVE-2023-52530, CVE-2023-52578, CVE-2023-52639, CVE-2023-52667, CVE-2023-6356, CVE-2023-6535, CVE-2023-6536, CVE-2024-1086, CVE-2024-1132 CVE-2024-25742, CVE-2024-25743, CVE-2024-26586, CVE-2024-26598, CVE-2024-26602, CVE-2024-26642)
Description	Red Hat has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to cause Use After Free, NULL pointer dereference, Path Transversal. Red Hat advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Red Hat CodeReady Linux Builder for ARM 64 - Extended Update Support 8.8 aarch64 Red Hat CodeReady Linux Builder for ARM 64 - Extended Update Support 9.2 aarch64 Red Hat CodeReady Linux Builder for IBM z Systems - Extended Update Support 9.2 s390x Red Hat CodeReady Linux Builder for Power, little endian - Extended Update Support 8.8 ppc64le Red Hat CodeReady Linux Builder for Power, little endian - Extended Update Support 9.2 ppc64le Red Hat CodeReady Linux Builder for x86_64 - Extended Update Support 8.8 x86_64 Red Hat CodeReady Linux Builder for x86_64 - Extended Update Support 9.2 x86_64 Red Hat Enterprise Linux for ARM 64 - Extended Update Support 8.8 aarch64 Red Hat Enterprise Linux for ARM 64 - Extended Update Support 9.2 aarch64 Red Hat Enterprise Linux for IBM z Systems - Extended Update Support 8.8 s390x and 9.2 s390x Red Hat Enterprise Linux for Power, little endian - Extended Update Support 8.8 ppc64le Red Hat Enterprise Linux for Power, little endian - Extended Update Support 9.2 ppc64le Red Hat Enterprise Linux for Real Time for NFV for x86_64 - 4 years of updates 9.2 x86_64 Red Hat Enterprise Linux for Real Time for x86_64 - 4 years of updates 9.2 x86_64 Red Hat Enterprise Linux for x86_64 - Extended Update Support 8.8 x86_64 Red Hat Enterprise Linux for x86_64 - Extended Update Support 9.2 x86_64 Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 8.4 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 9.2 x86_64 Red Hat Enterprise Linux Server - AUS 8.6 x86_64 and AUS 9.2 x86_64 Red Hat Enterprise Linux Server - TUS 8.6 x86_64 and TUS 8.8 x86_64 Red Hat Enterprise Linux Server for ARM 64 - 4 years of updates 9.2 aarch64 Red Hat Enterprise Linux Server for IBM z Systems - 4 years of updates 9.2 s390x Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 8.4 ppc64le 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 9.2 ppc64le Red Hat JBoss Middleware Text-Only Advisories for MIDDLEWARE 1 x86_64
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://access.redhat.com/errata/RHSA-2024:3859 • https://access.redhat.com/errata/RHSA-2024:3855 • https://access.redhat.com/errata/RHSA-2024:3854 • https://access.redhat.com/errata/RHSA-2024:3810 • https://access.redhat.com/errata/RHSA-2024:3752 • https://access.redhat.com/errata/RHSA-2024:3762 • https://access.redhat.com/errata/RHSA-2024:3805

Affected Product	**HPE**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-48795, CVE-2023-51385, CVE-2022-23829)
Description	HPE has released security updates addressing multiple vulnerabilities that exist in their products. Exploitation of these vulnerabilities may lead to Denial of Service (DoS), Disclosure of Information, Arbitrary Code Execution, Directory Traversal, Server-Side Request Forgery (SSRF). HPE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	HPE Aruba Networking AirWave Management Platform 8.3.0.2 and below HPE ProLiant DL325 Gen10 Plus server - Prior to v3.10_05-16-2024 HPE ProLiant DL325 Gen10 Plus v2 server - Prior to v3.10_05-16-2024 HPE ProLiant DL345 Gen10 Plus server - Prior to v3.10_05-16-2024 HPE ProLiant DL365 Gen10 Plus server - Prior to v3.10_05-16-2024 HPE ProLiant DL385 Gen10 Plus server - Prior to v3.10_05-16-2024 HPE ProLiant DL385 Gen10 Plus v2 server - Prior to v3.10_05-16-2024 HPE ProLiant XL225n Gen10 Plus 1U Node - Prior to v3.10_05-16-2024 HPE ProLiant DL325 Gen10 Server - Prior to v3.10_05-16-2024 HPE ProLiant DL385 Gen10 Server - Prior to v3.10_05-16-2024
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbhf04638en_us&docLocale=en_US • https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbnw04658en_us&docLocale=en_US

Affected Product	**SAP**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-37177, CVE-2024-34688, CVE-2024-33001, CVE-2024-34683, CVE-2024-34691, CVE-2024-34686, CVE-2024-32733, CVE-2024-37176, CVE-2024-34690, CVE-2024-28164, CVE-2024-34684, CVE-2024-33000)
Description	SAP has issued monthly security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited to cause Denial of Service, Information Disclosure, Unrestricted file upload, Cross-Site Scripting. SAP advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	SAP Financial Consolidation, Version - FINANCE 1010 SAP NetWeaver AS Java, Version - MMR_SERVER 7.5 SAP NetWeaver and ABAP platform, Versions - ST-PI 2008_1_700, 2008_1_710, 740 SAP Document Builder, Versions - S4CORE 100, 101, S4FND 102, 103, 104, 105, 106, 107, 108, SAP_BS_FND 702, 731, 746, 747, 748 SAP S/4HANA (Manage Incoming Payment Files), Versions – S4CORE 102, 103, 104, 105, 106, 107, 108 SAP CRM WebClient UI, Versions – S4FND 102, 103, 104, 105, 106, 107, WEBCUIF 700, 701, 730, 731, 746, 747, 748, 800, 801 SAP NetWeaver Application Server ABAP and ABAP Platform, Versions - SAP_BASIS 740, SAP_BASIS 750, SAP_BASIS 751, SAP_BASIS 752, SAP_BASIS 753, SAP_BASIS 754, SAP_BASIS 755, SAP_BASIS 756, SAP_BASIS 757, SAP_BASIS 758, SAP_BASIS 795, SAP_BASIS 796 SAP BW/4HANA Transformation and Data Transfer Process, Versions – DW4CORE 200, 300, 400, 796, SAP_BW 740, 750, 751, 752, 753, 754, 755, 756, 757, 758 SAP Student Life Cycle Management, Versions – IS-PS-CA 617, 618, 802, 803, 804, 805, 806, 807, 808 SAP NetWeaver AS Java, Version – GP-CORE 7.5 Central Finance Infrastructure Components, Versions - SAP_FIN 720, 730, SAPSCORE 114, S4CORE 100, 101, 102 SAP BusinessObjects Business Intelligence Platform, Versions – ENTERPRISE 420, 430, 440 SAP Bank Account Management, Versions – 100, 101, 102, 103, 104, 105, 106, 107, 108
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.sap.com/en/my-support/knowledge-base/security-notes-news/june-2024.html

Affected Product	**Ubuntu**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities
Description	Ubuntu has released security updates addressing multiple vulnerabilities that exist in their products. Exploitation of these vulnerabilities could lead to Denial of service, User after free conditions, Null pointer deference, Integer overflow. Ubuntu advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Ubuntu 24.04
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://ubuntu.com/security/notices/USN-6817-2

Disclaimer

The information provided herein is on "as is" basis, without warranty of any kind. FinCSIRT highly recommend to follow the company policies and procedures when applying the necessary patches with thorough testing and ensuring proper roll-back capabilities exists.