TLP: WHITE

Advisory Alert

Alert Number: AAA20240214 **Date:** February 14, 2024

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Microsoft	**Critical**	Multiple Vulnerabilities
Intel	**Critical**	Privilege Escalation Vulnerability
Intel	**High**, **Medium**, **Low**	Multiple Vulnerabilities
Lenovo	**High**, **Medium**, **Low**	Multiple Vulnerabilities
HPE	**High**, **Medium**, **Low**	Multiple Vulnerabilities
Fortiguard	**Medium**	Improper Neutralization Vulnerability

Description

Affected Product	**Microsoft**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-20667, CVE-2024-20673, CVE-2024-20679, CVE-2024-20684, CVE-2024-20695, CVE-2024-21304, CVE-2024-21315, CVE-2024-21327, CVE-2024-21328, CVE-2024-21329, CVE-2024-21338, CVE-2024-21339, CVE-2024-21340, CVE-2024-21341, CVE-2024-21342, CVE-2024-21343, CVE-2024-21344, CVE-2024-21345, CVE-2024-21346, CVE-2024-21347, CVE-2024-21348, CVE-2024-21349, CVE-2024-21350, CVE-2024-21351, CVE-2024-21352, CVE-2024-21353, CVE-2024-21354, CVE-2024-21355, CVE-2024-21356, CVE-2024-21357, CVE-2024-21358, CVE-2024-21359, CVE-2024-21360, CVE-2024-21361, CVE-2024-21362, CVE-2024-21363, CVE-2024-21364, CVE-2024-21365, CVE-2024-21366, CVE-2024-21367, CVE-2024-21368, CVE-2024-21369, CVE-2024-21370, CVE-2024-21371, CVE-2024-21372, CVE-2024-21374, CVE-2024-21375, CVE-2024-21376, CVE-2024-21377, CVE-2024-21378, CVE-2024-21379, CVE-2024-21380, CVE-2024-21381, CVE-2024-21384, CVE-2024-21386, CVE-2024-21389, CVE-2024-21391, CVE-2024-21393, CVE-2024-21394, CVE-2024-21395, CVE-2024-21396, CVE-2024-21397, CVE-2024-21399, CVE-2024-21401, CVE-2024-21402, CVE-2024-21403, CVE-2024-21404, CVE-2024-21405, CVE-2024-21406, CVE-2024-21410, CVE-2024-21412, CVE-2024-21413, CVE-2024-21420)
Description	Microsoft has released critical security updates for February 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 your systems from potential threats
Affected Products	.NET Azure Active Directory Azure Connected Machine Agent Azure DevOps Azure File Sync Azure Site Recovery Azure Stack Internet Shortcut Files Microsoft ActiveX Microsoft Azure Kubernetes Service Microsoft Defender for Endpoint Microsoft Dynamics Microsoft Edge (Chromium-based) Microsoft Exchange Server Microsoft Office Microsoft Office OneNote Microsoft Office Outlook Microsoft Office Word Microsoft Teams for Android Microsoft WDAC ODBC Driver Microsoft WDAC OLE DB provider for SQL Microsoft Windows Windows Server Microsoft Windows DNS Role: DNS Server Skype for Business SQL Server Trusted Compute Base Windows Hyper-V Windows Internet Connection Sharing (ICS) Windows Kernel Windows LDAP - Lightweight Directory Access Protocol Windows Message Queuing Windows OLE Windows SmartScreen Windows USB Serial Driver Windows Win32K - ICOMP
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://msrc.microsoft.com/update-guide/releaseNote/2024-Feb

Affected Product	**Intel**
Severity	**Critical**
Affected Vulnerability	Privilege Escalation Vulnerability (CVE-2023-31273)
Description	Intel has released a security update addressing a Privilege escalation vulnerability that exists in their products. The vulnerability is due to a failure in the protection mechanism of the Intel Data Center Manager (DCM) software. Intel strongly recommends to apply the necessary patch updates at your earliest to avoid issues
Affected Products	Intel Data Center Manager software before version 5.2.
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00902.html

Affected Product	**Intel**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities
Description	Intel has released security updates addressing multiple vulnerabilities that exist in their products. These releases include fixes for multiple BIOS and Firmware products. Intel recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	Multiple Products
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.intel.com/content/www/us/en/security-center/default.html

Affected Product	**Lenovo**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-31271, CVE-2023-32646, CVE-2023-34315, CVE-2023-41252, CVE-2024-21982, CVE-2021-38575, CVE-2021-38576, CVE-2021-38578, CVE-2021-42299, CVE-2023-20576, CVE-2023-20577, CVE-2023-20579, CVE-2023-20587, CVE-2023-25174, CVE-2023-28388, CVE-2023-28739, CVE-2023-29153, CVE-2023-31346, CVE-2023-31347, CVE-2023-34469, CVE-2023-34470, CVE-2023-35841, CVE-2023-45229, CVE-2023-45230, CVE-2023-45231, CVE-2023-45232, CVE-2023-45233, CVE-2023-45234, CVE-2023-45235, CVE-2024-23591, CVE-2023-4969, CVE-2023-45779, CVE-2023-33870, CVE-2023-39432, CVE-2023-33875, CVE-2023-28720, CVE-2023-32642, CVE-2023-34983, CVE-2023-35061, CVE-2023-28374, CVE-2023-25951, CVE-2023-26586, CVE-2023-32651, CVE-2023-32644, CVE-2023-22293, CVE-2023-25777, CVE-2023-22342, CVE-2023-25779, CVE-2023-24542, CVE-2023-22390, CVE-2023-24481, CVE-2023-24589, CVE-2023-22848, CVE-2023-25769, CVE-2023-26585, CVE-2023-27308, CVE-2023-24463, CVE-2023-27301, CVE-2023-27307, CVE-2023-27300, CVE-2023-26592, CVE-2023-27303, CVE-2023-26596, CVE-2023-26591)
Description	Lenovo has released security updates addressing multiple vulnerabilities that exist in their products. An attacker may exploit these vulnerabilities to cause Arbitrary Code Execution, Denial of Service, Privilege Escalation, and Information Disclosure. Lenovo recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	Multiple Products
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.lenovo.com/us/en/product_security/LEN-154269 https://support.lenovo.com/us/en/product_security/LEN-152496 https://support.lenovo.com/us/en/product_security/LEN-150741 https://support.lenovo.com/us/en/product_security/LEN-150692 https://support.lenovo.com/us/en/product_security/LEN-150020 https://support.lenovo.com/us/en/product_security/LEN-149654 https://support.lenovo.com/us/en/product_security/LEN-148889 https://support.lenovo.com/us/en/product_security/LEN-147238 https://support.lenovo.com/us/en/product_security/LEN-145288 https://support.lenovo.com/us/en/product_security/LEN-137494 https://support.lenovo.com/us/en/product_security/LEN-124490

Affected Product	**HPE**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-23583, 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-2023-20577, CVE-2023-20587, CVE-2023-31346, CVE-2023-31347)
Description	HPE has released security updates addressing multiple vulnerabilities that exist in their products. Exploitation of these vulnerabilities may cause escalation of privilege, information disclosure, denial of service, arbitrary code execution. HPE recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	HPE ProLiant DL325 Gen10 Plus server - Prior to v3.00_01_26_2024 HPE ProLiant DL325 Gen10 Plus v2 server - Prior to v3.00_01_26_2024 HPE ProLiant DL325 Gen11 Server - Prior to v1.58_01_04_2024 HPE ProLiant DL345 Gen10 Plus server - Prior to v3.00_01_26_2024 HPE ProLiant DL345 Gen11 Server - Prior to v1.58_01_04_2024 HPE ProLiant DL365 Gen10 Plus server - Prior to v3.00_01_26_2024 HPE ProLiant DL365 Gen11 Server - Prior to v1.58_01_04_2024 HPE ProLiant DL385 Gen10 Plus server - Prior to v3.00_01_26_2024 HPE ProLiant DL385 Gen10 Plus v2 server - Prior to v3.00_01_26_2024 HPE ProLiant DL385 Gen10 Server - Prior to v3.00_01_26_2024 HPE ProLiant DL385 Gen11 Server - Prior to v1.58_01_04_2024 HPE ProLiant DX325 Gen10 Plus v2 server - Prior to v3.00_01_26_2024 HPE ProLiant DX365 Gen11 Server - Prior to v1.58_01_04_2024 HPE ProLiant DX385 Gen10 Plus server - Prior to v3.00_01_26_2024 HPE ProLiant DX385 Gen10 Plus v2 server - Prior to v3.00_01_26_2024 HPE ProLiant DX385 Gen11 Server - Prior to v1.58_01_04_2024 HPE ProLiant XL225n Gen10 Plus 1U Node - Prior to v3.00_01_26_2024 HPE ProLiant XL645d Gen10 Plus Server - Prior to v3.00_01_26_2024 HPE ProLiant XL675d Gen10 Plus Server - Prior to v3.00_01_26_2024 HPE SimpliVity 380 Gen10 Plus - Prior to HPE OmniStack Firmware Version 2024_0131
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04566en_us https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04594en_us https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04591en_us https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04592en_us

Affected Product	**Fortiguard**
Severity	**Medium**
Affected Vulnerability	Improper Neutralization Vulnerability (CVE-2023-26206)
Description	Fortiguard has released security updates addressing an Improper Neutralization vulnerability that exists in FortiNAC. Exploitation of this vulnerability may allow a remote unauthenticated attacker to perform a stored cross site scripting (XSS) attack via the name fields observed in the policy audit logs. Fortiguard recommends to apply the necessary software updates to avoid issue
Affected Products	FortiNAC 9.4.0 through 9.4.3 FortiNAC 9.2 all versions FortiNAC 9.1 all versions FortiNAC 8.8 all versions FortiNAC 8.7 all versions FortiNAC 8.6 all versions FortiNAC 8.5 all versions FortiNAC 8.3 all versions FortiNAC 7.2.0 through 7.2.2
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.fortiguard.com/psirt/FG-IR-23-063

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.