Advisory Alert

Alert Number: **AAA20230619** **Date:** **June 19, 2023**

Document Classification Level **:** Public Circulation Permitted | Public

Information Classification Level **:** TLP: WHITE

Overview

Product	Severity	Vulnerability
Microsoft	**High**	Multiple Remote Code Execution Vulnerabilities
Ubuntu	**High, Medium**	Multiple Vulnerabilities
Cisco	**Medium**	Information Disclosure Vulnerability
Fortinet	**Medium**	NULL pointer dereference vulnerability

Description

Affected Product	**Microsoft**
Severity	**High**
Affected Vulnerability	Multiple Remote Code Execution Vulnerabilities (CVE-2023-32025, CVE-2023-32026, CVE-2023-32027, CVE-2023-32028, CVE-2023-29349, CVE-2023-29356)
Description	Microsoft has released security updates addressing Multiple Remote Code Execution Vulnerabilities in SQL Server. Microsoft recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	Microsoft ODBC Driver 17 for SQL Server on Windows Microsoft ODBC Driver 18 for SQL Server on Linux Microsoft ODBC Driver 18 for SQL Server on Windows Microsoft ODBC Driver 17 for SQL Server on MacOS Microsoft ODBC Driver 18 for SQL Server on MacOS Microsoft ODBC Driver 17 for SQL Server on Linux Microsoft SQL Server 2019 for x64-based Systems (CU 21) Microsoft SQL Server 2022 for x64-based Systems (CU 5) Microsoft OLE DB Driver 18 for SQL Server Microsoft OLE DB Driver 19 for SQL Server
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32025 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32026 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32027 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32028 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-29349 https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-29356

Affected Product	**Ubuntu**
Severity	**High, Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-4269, CVE-2023-1076, CVE-2023-1077, CVE-2023-1079, CVE-2023-1380, CVE-2023-1583, CVE-2023-1611, CVE-2023-1670, CVE-2023-1855, CVE-2023-1859, CVE-2023-1989, CVE-2023-1990, CVE-2023-1998, CVE-2023-2002, CVE-2023-2156, CVE-2023-2194, CVE-2023-2235, CVE-2023-2269, CVE-2023-25012, CVE-2023-2612, CVE-2023-28466, CVE-2023-28866, CVE-2023-2985, CVE-2023-30456, CVE-2023-30772, CVE-2023-31436, CVE-2023-32233, CVE-2023-32250, CVE-2023-32254, CVE-2023-33203, CVE-2023-33288)
Description	Ubuntu has released security updates addressing Multiple Vulnerabilities in their products. If exploited theses vulnerabilities could lead to denial of service, sensitive information disclosure and arbitrary code execution. Ubuntu recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	Ubuntu 20.04 Ubuntu 22.04 Ubuntu 22.10 Ubuntu 23.04
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://ubuntu.com/security/notices/USN-6175-1 https://ubuntu.com/security/notices/USN-6173-1 https://ubuntu.com/security/notices/USN-6172-1 https://ubuntu.com/security/notices/USN-6171-1

Affected Product	**Cisco**
Severity	**Medium**
Affected Vulnerability	Information Disclosure Vulnerability (CVE-2021-1546)
Description	Cisco has released a security update addressing an Information Disclosure Vulnerability in the CLI of Cisco SD-WAN software. A local authenticated attacker could exploit this vulnerability by running a CLI command that targets an arbitrary file on the local system. If exploited, attackers could return portions of an arbitrary file, resulting in sensitive information disclosure. Cisco recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	Cisco SD-WAN Software Release 20.3, 20.4, 20.5, 20.6 on following products • SD-WAN vBond Orchestrator Software • SD-WAN vEdge Cloud Routers • SD-WAN vEdge Routers • SD-WAN vManage Software • SD-WAN vSmart Controller Software
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sd-wan-Fhqh8pKX

Affected Product	**Fortinet**
Severity	**Medium**
Affected Vulnerability	NULL pointer dereference vulnerability (CVE-2023-33306)
Description	Fortinet has released a security update addressing a NULL pointer dereference vulnerability in the FortiOS and FortiProxy. A authenticated remote attacker could exploit this vulnerability by sending crafted request to the NULL pointer dereference in SSL-VPN to trigger crash of SSL-VPN. Fortinet recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	FortiOS version 7.2.0 through 7.2.4 FortiOS version 7.0.0 through 7.0.10 FortiProxy version 7.2.0 through 7.2.2 FortiProxy version 7.0.0 through 7.0.8
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.fortiguard.com/psirt/FG-IR-23-015

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.