Advisory Alert

Alert Number: AAA20231025 **Date:** October 25, 2023

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
VMware	**Critical**	Multiple Vulnerabilities
IBM	**Critical**	Multiple Vulnerabilities
Suse	**High**	Multiple Vulnerabilities
Ubuntu	**High**, Medium , Low	Multiple Vulnerabilities
IBM	**High**, Medium , Low	Multiple Vulnerabilities
OpenSSL	Medium	Incorrect cipher key & IV length processing

Description

Affected Product	**VMware**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-34048, CVE-2023-34056)
Description	VMware has released a critical security update addressing multiple vulnerabilities in VMware vCenter Server and Cloud Foundation that could lead to out-of-bounds write and information disclosure **CVE-2023-34048 -** A malicious actor with network access to vCenter Server may trigger an out-of-bounds write potentially leading to remote code execution due to a vulnerability in the implementation of the DCERPC protocol. **CVE-2023-34056-** vCenter Server contains a partial information disclosure vulnerability. A malicious actor with non-administrative privileges to vCenter Server may leverage this issue to access unauthorized data. VMware highly recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	VMware vCenter Server 8.0 VMware vCenter Server 7.0 VMware Cloud Foundation (VMware vCenter Server) 5.x, 4.x
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.vmware.com/security/advisories/VMSA-2023-0023.html

Affected Product	**IBM**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-25147, CVE-2016-1000027)
Description	IBM has released a critical security update addressing multiple vulnerabilities in IBM QRadar SIEM that could lead to arbitrary code execution and denial of service. **CVE-2022-25147-** Arbitrary code execution vulnerability exist in Apache Portable Runtime caused by an integer overflow in the apr_base64 functions. An attacker could exploit this vulnerability by sending a specially-crafted request to execute arbitrary code and cause denial of service. **CVE-2016-1000027 -** Arbitrary code execution vulnerability exist in Pivota Spring Framework caused by an unsafe deserialization flaw in the library. Remote attacker could exploit this vulnerability by sending a specially-crafted input. IBM highly recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	IBM QRadar SIEM version 7.5.0 - 7.5.0 UP6
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7049133

Affected Product	**Suse**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-3390 ,CVE-2023-4004, CVE-2023-4147, CVE-2023-4623)
Description	Suse has released security updates addressing Multiple Vulnerabilities in their products. Successful exploitation of these vulnerabilities could lead to local privilege escalation. Suse recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	openSUSE Leap 15.5 SUSE Linux Enterprise High Performance Computing 15 SP4 SUSE Linux Enterprise High Performance Computing 15 SP5 SUSE Linux Enterprise Live Patching 15-SP4 SUSE Linux Enterprise Live Patching 15-SP5 SUSE Linux Enterprise Micro 5.3 SUSE Linux Enterprise Micro 5.4 SUSE Linux Enterprise Micro 5.5 SUSE Linux Enterprise Real Time 15 SP4 SUSE Linux Enterprise Real Time 15 SP5 SUSE Linux Enterprise Server 15 SP4 SUSE Linux Enterprise Server 15 SP5 SUSE Linux Enterprise Server for SAP Applications 15 SP4 SUSE Linux Enterprise Server for SAP Applications 15 SP5
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.suse.com/support/update/announcement/2023/suse-su-20234166-1/ https://www.suse.com/support/update/announcement/2023/suse-su-20234165-1/ https://www.suse.com/support/update/announcement/2023/suse-su-20234164-1/

Affected Product	**Ubuntu**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-42756, CVE-2023-5197, CVE-2023-4244, CVE-2023-4921, CVE-2023-4881, CVE-2023-42752, CVE-2023-42755, CVE-2023-4622, CVE-2023-4623, CVE-2023-34319, CVE-2023-42753, CVE-2023-38432, CVE-2023-20569, CVE-2023-3338, CVE-2023-4273, CVE-2023-2156, CVE-2023-4155, CVE-2023-3866, CVE-2023-3865, CVE-2023-3863, CVE-2023-4132, CVE-2023-1206, CVE-2023-4194, CVE-2023-44466)
Description	Ubuntu has released security update addressing Multiple Vulnerabilities in Ubuntu 20.04. Successful exploitation of these vulnerabilities could lead to Denial of Service, sensitive information disclosure, Arbitrary code Execution. Ubuntu recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	Ubuntu 20.04 LTS
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://ubuntu.com/security/notices/USN-6445-2 https://ubuntu.com/security/notices/USN-6446-2 https://ubuntu.com/security/notices/USN-6444-2

Affected Product	**IBM**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-34981, CVE-2020-13956, CVE-2023-21830, CVE-2023-21843, CVE-2022-3564, CVE-2023-32067, CVE-2023-33201, CVE-2023-28709, CVE-2023-30441, CVE-2023-40367, CVE-2023-34455, CVE-2023-34454, CVE-2023-34453, CVE-2022-40609, CVE-2022-48339, CVE-2023-35116, CVE-2023-20867, CVE-2022-21426, CVE-2023-26048, CVE-2023-26049, CVE-2023-30994, CVE-2023-38408, CVE-2023-2828, CVE-2023-34149, CVE-2023-25652, CVE-2023-29007, CVE-2023-32697, CVE-2023-21930, CVE-2023-21967, CVE-2023-21954, CVE-2023-21939, CVE-2023-21968, CVE-2023-21937, CVE-2023-21938, CVE-2023-2597, CVE-2023-2976, CVE-2023-34396, CVE-2023-31484, CVE-2023-31486)
Description	IBM has released security updates addressing Multiple Vulnerabilities in their products .Successful exploitation of above vulnerabilities could lead to sensitive information disclosure, arbitrary code execution, denial of service IBM recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	IBM QRadar SIEM version 7.5.0 - 7.5.0 UP6 IBM WebSphere Hybrid Edition Version 5.1 IBM WebSphere Application Server Liberty Version 23.0.0.9 - 23.0.0.10 AIX Version 7.2 AIX Version 7.3 VIOS Version 3.1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7049133 https://www.ibm.com/support/pages/node/7058536 https://www.ibm.com/support/pages/node/7058356 https://www.ibm.com/support/pages/node/7047272

Affected Product	**OpenSSL**
Severity	**Medium**
Affected Vulnerability	Incorrect cipher key & IV length processing (CVE-2023-5363)
Description	OpenSSL has released a security update addressing Incorrect cipher key & IV length processing flow in their products which can lead to potential truncation or overruns during the initialization of some symmetric ciphers. Successful exploitation of this vulnerability could lead to sensitive information disclosure OpenSSL recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	OpenSSL 3.0 OpenSSL 3.1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.openssl.org/news/secadv/20231024.txt

Disclaimer