Advisory Alert

Alert Number: AAA20230503 **Date:** May 3, 2023

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Juniper	**High**	Multiple Vulnerabilities
Ubuntu	**High**, **Medium**, **Low**	Multiple Vulnerabilities
IBM	**Medium**	Spoofing Vulnerability

Description

Affected Product	**Juniper**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2017-6460, CVE-2017-6459, CVE-2017-6458, CVE-2017-6455, CVE-2017-6452, CVE-2017-6451, CVE-2016-9312, CVE-2016-9311, CVE-2016-9310, CVE-2016-9042, CVE-2016-7434, CVE-2016-7433, CVE-2016-7431, CVE-2016-7429, CVE-2016-7428, CVE-2016-7427, CVE-2016-7426, CVE-2016-4957, CVE-2016-4956, CVE-2016-4955, CVE-2016-4954, CVE-2016-4953, CVE-2016-2519, CVE-2016-2518, CVE-2016-2517, CVE-2016-2516, CVE-2016-1551, CVE-2016-1550, CVE-2016-1548, CVE-2016-1547, CVE-2015-8158, CVE-2015-8140, CVE-2015-8139, CVE-2015-8138, CVE-2015-7979, CVE-2015-7978, CVE-2015-7977, CVE-2015-7976, CVE-2015-7975, CVE-2015-7974, CVE-2015-7973, CVE-2015-5146, CVE-2013-5211)
Description	Juniper has released security updates addressing multiple vulnerabilities that exist in products or platforms running Junos OS with NTP services enabled. If exploited these vulnerabilities could lead to Buffer overflow, Denial of service, Privilege escalation, Out-of-bounds memory writ, Impersonation attack and Man in the Middle (MITM) attack. Juniper recommends to apply necessary security fixes at earliest to avoid issues
Affected Products	Juniper Networks Junos OS 12.3 versions prior to 12.3R12-S15 on EX Series; Juniper Networks Junos OS 12.3X48 versions prior to 12.3X48-D95 on SRX Series; Juniper Networks Junos OS 14.1X53 versions prior to 14.1X53-D53; Juniper Networks Junos OS 15.1 versions prior to 15.1R7-S6 on EX Series; Juniper Networks Junos OS 15.1X49 versions prior to 15.1X49-D190 on SRX Series; Juniper Networks Junos OS 16.1 versions prior to 16.1R7-S6; Juniper Networks Junos OS 16.2 versions prior to 16.2R3; Juniper Networks Junos OS 17.1 versions prior to 17.1R2-S11, 17.1R3-S1; Juniper Networks Junos OS 17.2 versions prior to 17.2R1-S9, 17.2R2-S8, 17.2R3-S3; Juniper Networks Junos OS 17.3 versions prior to 17.3R2-S5, 17.3R3-S6; Juniper Networks Junos OS 17.4 versions prior to 17.4R2-S7, 17.4R3; Juniper Networks Junos OS 18.1 versions prior to 18.1R3-S8; Juniper Networks Junos OS 18.2 versions prior to 18.2R2-S7, 18.2R3-S1; Juniper Networks Junos OS 18.3 versions prior to 18.3R1-S5, 18.3R2-S2, 18.3R3; Juniper Networks Junos OS 18.4 versions prior to 18.4R1-S4, 18.4R2-S1, 18.4R3; Juniper Networks Junos OS 19.1 versions prior to 19.1R1-S3, 19.1R2; Juniper Networks Junos OS 19.2 versions prior to 19.2R1-S1, 19.2R2. Juniper Networks Junos OS Evolved All versions prior to 20.1R1-EVO
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://supportportal.juniper.net/s/article/2021-04-Security-Bulletin-Junos-OS-and-Junos-OS-Evolved-Multiple-NTP-vulnerabilities-resolved?language=en_US https://supportportal.juniper.net/s/article/2017-04-Security-Bulletin-Junos-Multiple-vulnerabilities-in-NTP-VU-633847?language=en_US

Affected Product	**Ubuntu**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-1829, CVE-2023-1872, CVE-2022-3586, CVE-2023-1670, CVE-2023-1390, CVE-2022-4095)
Description	Ubuntu has released security updates addressing multiple vulnerabilities that exists in their products. Successful exploitation of these vulnerabilities could lead to Denial of Service and Privilege escalation. Ubuntu recommends to apply necessary security fixes at earliest to avoid issues.
Affected Products	Ubuntu 14.04 Ubuntu 16.04 Ubuntu 20.04 Ubuntu 22.04
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://ubuntu.com/security/notices/USN-6044-1 https://ubuntu.com/security/notices/USN-6045-1

Affected Product	**IBM**
Severity	**Medium**
Affected Vulnerability	Spoofing Vulnerability (CVE-2022-39161)
Description	IBM has released security updates addressing a Spoofing vulnerability that exist in IBM WebSphere Application Server. An authenticated user could conduct spoofing attacks when IBM WebSphere Application Server and IBM WebSphere Application Server Liberty are configured to communicate with the Web Server Plug-ins for IBM WebSphere Application Server. A man-in-the-middle attacker could exploit this vulnerability using a certificate issued by a trusted authority to obtain sensitive information. IBM recommends to apply necessary security fixes at earliest to avoid issues.
Affected Products	IBM WebSphere Hybrid Edition 5.1 IBM WebSphere Application Server 9.0, 8.5 with Web Server Plug-ins 9.0, 8.5 IBM WebSphere Application Server Liberty with Web Server Plug-ins 17.0.0.3 - current
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/6987829 https://www.ibm.com/support/pages/node/6987825 https://www.ibm.com/support/pages/node/6987779

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.