Advisory Alert

Alert Number: AAA20221006 **Date:** October 6, 2022

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
IBM	**Critical**	Arbitrary Code Execution Vulnerability
IBM	**High**, **Medium**	Multiple Vulnerabilities
Cisco	**High**, **Medium**	Multiple Vulnerabilities
RedHat	**High**	Multiple Denial of Service Vulnerabilities

Description

Affected Product	**IBM**
Severity	**Critical**
Affected Vulnerability	Arbitrary Code Execution Vulnerability (CVE-2022-40674)
Description	IBM has released a Security Update addressing an Arbitrary code execution vulnerability in the Expact library that used in their IBM HTTP Server that used by IBM WebSphere Application Server .The Expat library is used by IBM HTTP Server's WebDAV (mod_dav) support, but may also be used by third-party Apache HTTP Server modules if they have been loaded into the server by the administrator. An attacker could exploit this vulnerability to execute arbitrary code on the system. IBM highly recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	IBM HTTP Server 9.0, 8.5, 8.0, 7.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/6827119

Affected Product	**IBM**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-31129, CVE-2022-24785, CVE-2017-18214, CVE-2022-22480)
Description	IBM has released security updates addressing multiple vulnerabilities that exists in IBM QRadar DNS Analyzer App and IBM QRadar SIEM. **CVE-2022-31129**- Denial of service vulnerability that caused by inefficient regular expression complexity of the moment.js that is used in the IBM QRadar DNS Analyzer App for IBM QRadar SIEM . A remote attacker can exploit this vulnerability by sending a specially-crafted request. **CVE-2022-24785**- Directory traversal vulnerability that caused by improper validation of user supplied input in the Moment.js that is used in the IBM QRadar DNS Analyzer App for IBM QRadar SIEM. Using this vulnerability an attacker can switch arbitrary moment locale by sending a specially-crafted locale string containing "dot dot" sequences (/../) **CVE-2017-18214**- A denial of service vulnerability exist in the Node.js moment module. A remote attacker could exploit this vulnerability to cause a low severity regular expression denial of service. **CVE-2022-22480**-An information disclosure vulnerability that exists because IBM QRadar SIEM data node rebalancing does not function correctly when using encrypted hosts. IBM highly recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	IBM QRadar SIEM 7.4.0 - 7.4.3 Fix Pack 6 IBM QRadar SIEM 7.5.0 - 7.5.0 Update Pack 2 IBM QRadar DNS Analyzer App 1.0 - 2.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/6827213 https://www.ibm.com/support/pages/node/6826695

Affected Product	**Cisco**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities(CVE-2022-20814, CVE-2022-20853, CVE-2022-20929, CVE-2021-27853, CVE-2021-27854, CVE-2021-27861, CVE-2021-27862, CVE-2022-20952, CVE-2022-20917, CVE-2022-20939, CVE-2022-20948, CVE-2022-20686, CVE-2022-20687, CVE-2022-20688, CVE-2022-20689, CVE-2022-20690, CVE-2022-20691, CVE-2022-20766, CVE-2022-20793, CVE-2022-20931)
Description	Cisco has released security updates addressing multiple vulnerabilities that exists in their products. Exploitation of most severe vulnerabilities could cause cross-site request forgery, certificate validation bypass, network security control bypass, bypass configured first-hop security (FHS), rule bypass, manipulation of XMPP messages, privilege escalation, arbitrary code execution and Insufficient Identity Verification. Cisco highly recommends to apply the necessary patch updates at your earliest to avoid issues
Affected Products	Cisco Expressway Series and Cisco TelePresence VCS Release 14.0 and prior versions Cisco Enterprise NFVIS Release 4.0 and prior versions Cisco IOS Software Catalyst 6500 and 6800 Series Switches Cisco IOS Software Catalyst Digital Building Series Switches Cisco IOS Software Industrial Ethernet Switches Cisco IOS Software Micro Switches Cisco IOS XE Software Catalyst 4500 IOS-XE Switches Cisco IOS XE Software IOS XE Switches IOS XE Routers configured with Ethernet virtual circuits IOS XR Routers configured with L2 Transport services Cisco Meraki Switches - MS390, MS210, MS225, MS250, MS350, MS355, MS410, MS420, MS425, MS450 Nexus 3000 Series Switches Nexus 5500 Platform Switches Nexus 5600 Platform Switches Nexus 6000 Series Switches Nexus 7000 Series Switches Nexus 9000 Series Switches (Standalone Mode) Cisco Small Business 250 Series Smart Switches Cisco Small Business 350 Series Managed Switches Cisco Small Business 350X Series Stackable Managed Switches Cisco Small Business 550X Series Stackable Managed Switches Cisco Small Business 250 Series Smart Switches Cisco Small Business 350 Series Managed Switches Cisco Jabber for Windows Release 12.5 and prior, 12.6, 12.7, 12.8, 12.9, 14.0, 14.1 Cisco Jabber for MacOS Release 12.7 and earlier 12.8, 12.9, 14.0, 14.1 Cisco Jabber for Android and iOS Release 14.1 and prior versions Cisco Jabber for Android MAM Release 14.1 and prior versions Cisco Jabber for iOS MAM Release Earlier than 14.1 and 14.1 Cisco Secure Web Appliance virtual and hardware versions Cisco Smart Software Manager On-Prem Release Earlier than 8-202206 Cisco BroadWorks Hosted Thin Receptionist Software Release 22.0 and prior versions, 23.0, 24.0 Cisco products running a vulnerable release of Cisco ATA 190 Series On-Premises Software Cisco products running a vulnerable release of Cisco ATA 190 Series Multiplatform (MPP) Software Cisco TelePresence CE Software Cisco RoomOS Software in cloud-aware on-premises operation
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-expressway-csrf-sqpsSfY6 https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-NFVIS-ISV-BQrvEv2h https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-VU855201-J3z8CKTX https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-wsa-bypass-bwBfugek https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-jabber-xmpp-Ne9SCM https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cssm-priv-esc-SEjz69dv https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-bw-thinrcpt-xss-gSj4CecU https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ata19x-multivuln-GEZYVvs https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-CTT-IVV-4A66Dsfj https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-CTT-DAV-HSvEHHEt

Affected Product	**RedHat**
Severity	**High**
Affected Vulnerability	Multiple denial of service vulnerabilities (CVE-2022-1259, CVE-2022-2053, CVE-2022-25857)
Description	ReHat has released a security patch updates addressing a denial of service vulnerability that exists in their JBoss Enterprise Application Platform product. **CVE-2022-1259**- A flaw was found in Undertow. A potential security issue in flow control handling by the browser over HTTP/2 may cause overhead or a denial of service in the server. **CVE-2022-2053**- A flaw was found in Undertow. AJP requests to the server may allow an attacker to send a malicious request and trigger server errors, resulting in a denial of service. **CVE-2022-25857**- A flaw was found in the org.yaml.snakeyaml package. This flaw allows an attacker to cause a denial of service (DoS) due to missing nested depth limitation for collections. RedHat highly recommends to apply the necessary patch updates at your earliest to avoid issues
Affected Products	JBoss Enterprise Application Platform Text-Only Advisories x86_64
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2022:6825

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.