Advisory Alert

Alert Number: AAA20210308 **Date:** March 8, 2021

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Cisco	Critical, Medium	Multiple Vulnerabilities
IBM	High	Multiple Vulnerabilities

Description

Affected Product	Cisco
Severity	CVE-2021-1361 - Critical, CVE-2021-1425 - Medium
Affected Vulnerabilities	Multiple Vulnerabilities (CVE-2021-1361, CVE-2021-1425)
Description	Cisco has released Security Updates which addresses multiple Vulnerabilities across several products. **CVE-2021-1361** - A vulnerability in the implementation of an internal file management service for Cisco Nexus 3000 Series Switches and Cisco Nexus 9000 Series Switches in standalone NX-OS mode that are running Cisco NX-OS Software. The vulnerability exists due to the service at port 9075 is incorrectly configured to listen and respond to external connection requests. A remote non authenticated attacker can send specially crafted packets to port 9075 and create, delete, or overwrite arbitrary files on the system with root privileges. **CVE-2021-1425** - Cisco Email Security Appliance and Content Security Management Appliance could allow a remote authenticated attacker to obtain sensitive information, caused by a flaw in the web-based management interface. By looking at the raw HTTP requests that are sent to the interface, a remote attacker could exploit this vulnerability to obtain sensitive information.
Affected Products	Nexus 3000 Series Switches Nexus 9000 Series Switches in standalone NX-OS mode ESA – 13.5.1 and earlier SMA – earlier than 13.8.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-3000-9000-file-action-QtLzDRy2 https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-esa-sma-info-disclo-VOu2GHbZ

Affected Product	IBM
Severity	**High**
Affected Vulnerabilities	Multiple Vulnerabilities(CVE-2020-14803, CVE-2020-27221, CVE-2020-2773, CVE-2020-14781, CVE-2020-7692)
Description	IBM has released Security patch updates addressing multiple vulnerabilities that exists with multiple IBM products. IBM highly recommends to apply necessary fixes at earliest to avoid issues.
Affected Products	BIBM Java SDK shipped with IBM WebSphere Application Server Patterns 1.0.0.0 through 1.0.0.7 and 2.2.0.0 through 2.3.3.3. All GoogleCommon versions before 7.3.0-QRADAR-PROTOCOL-GoogleCommon-7.3-20210126200436 All GoogleCommon versions before 7.4.0-QRADAR-PROTOCOL-GoogleCommon-7.4-2021012620043
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/6425553 https://www.ibm.com/support/pages/node/6417571

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.