Advisory Alert

Alert Number: AAA20210211 **Date:** February 11, 2021

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Redhat	**High**	Denial of Service
Cisco	**High**	Sudo Privilege Escalation
IBM WebSphere Application Server	**High**	XML External Entity Injection (XXE)
IBM QRadar	**High**	Cross Site Scripting
Intel	**High**	Privilege Escalation, Information Disclosure

Description

Affected Product	Redhat
Severity	**High**
Affected Vulnerability	Denial of Service (CVE-2021-1721)
Description	Redhat has released security patch updates addressing a Denial of Service that exists in the dotnet. A recursion error when building X.509 certificate chains can lead to a stack overflow which could crash the system.
Affected Products	dotNET on RHEL (for RHEL Server) 1 x86_64 dotNET on RHEL (for RHEL Workstation) 1 x86_64 dotNET on RHEL (for RHEL Compute Node) 1 x86_64
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/security/cve/cve-2021-1721

Affected Product	Cisco
Severity	**High**
Affected Vulnerability	Sudo Privilege Escalation (CVE-2021-3156)
Description	Cisco has released a security patch update. Successful exploitation of this vulnerability allows any unprivileged user to gain root privileges and invoking the sudoedit command with crafted parameters or by executing a binary exploit.
Affected Products	Multiple Products
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sudo-privesc-jan2021-qnYQfcM#vulnerable

Affected Product	IBM WebSphere Application Server
Severity	**High**
Affected Vulnerability	XML External Entity Injection (XXE) (CVE-2021-20353)
Description	IBM WebSphere Application Server is vulnerable to an XML External Entity Injection (XXE) attack when processing XML data. A remote attacker could exploit this vulnerability to expose sensitive information or consume memory resources
Affected Products	WebSphere Application Server 9.0 WebSphere Application Server 8.5 WebSphere Application Server 8.0 WebSphere Application Server 7.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/6413709

Affected Product	IBM QRadar
Severity	**High**
Affected Vulnerability	Cross Site Scripting (CVE-2015-9251, CVE-2020-11022, CVE-2020-26870)
Description	IBM QRadar has released security patch updates. **CVE-2015-9251** - jQuery is vulnerable to Cross-site Scripting (XSS) attacks when a cross-domain Ajax request is performed without the dataType option, causing text/javascript responses to be executed. **CVE-2020-11022** - jQuery passing HTML from untrusted sources even after sanitizing it to one of jQuery's DOM manipulation methods may execute untrusted code. **CVE-2020-26870** - Cure53 DOMPurify allows mutation XSS. This occurs because a serialize-parse roundtrip does not necessarily return the original DOM tree, and a namespace can change from HTML to MathML, as demonstrated by the nesting of FORM elements.
Affected Products	IBM Security QRadar Analyst Workflow 1.0.0 - 1.4.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/6413705

Affected Product	Intel
Severity	**High**
Affected Vulnerability	Privilege Escalation (CVE-2020-12373, CVE-2020-12377, CVE-2020-12380, CVE-2020-12375) Information Disclosure (CVE-2020-12376)
Description	Security vulnerabilities in Intel some Server Boards, Server Systems and Compute Modules Baseboard Management Controller firmware may allow escalation of privilege or information disclosure. Intel is releasing firmware updates to mitigate these potential vulnerabilities.
Affected Products	Intel Server System R1000WF and R2000WF Families Intel Server Board S2600WF Family Intel Server Board S2600ST Family Intel Compute Module HNS2600BP Family Intel Server Board S2600BP Family
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00434.html

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.