Advisory Alert

Alert Number: AAA20210205 **Date:** February 5, 2021

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
SonicWall	**Critical**	SQL Injection vulnerability
Cisco	**High**	Multiple Vulnerabilities
IBM WebSphere	**Medium**	Directory Traversal Vulnerability
IBM QRadar SIEM	**Medium**	Denial of Service
Citrix	**Low**	Privilege Escalation

Description

Affected Product	**SonicWall**
Severity	**Critical**
Affected Vulnerability	SQL Injection vulnerability (CVE-2021-20016)
Description	Sonicwall has released security patch updates addressing SQL Injection vulnerability in the product allows a remote unauthenticated attacker to perform SQL query to access username password and other session related information.
Affected Products	SonicWall SMA 100 devices with v10.x firmware
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2021-0001

Affected Product	**Cisco**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2021-1288, CVE-2021-1313, CVE-2021-1289, CVE-2021-1290, CVE-2021-1291, CVE-2021-1268, CVE-2021-1136, CVE-2021-1244, CVE-2021-1370, CVE-2021-1221, CVE-2021-1243, CVE-2021-1389, CVE-2021-1296, CVE-2021-1297)
Description	Cisco has released Security Updates which address multiple Vulnerabilities across several of products. **CVE-2021-1288, CVE-2021-1313** - Ingress packet processing function of Cisco IOS XR Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device **CVE-2021-1289, CVE-2021-1290, CVE-2021-1291** - These vulnerabilities exist because HTTP requests are not properly validated. An attacker could exploit these vulnerabilities by sending a crafted HTTP request to the web-based management interface of an affected device **CVE-2021-1268 -** In the IPv6 protocol handling of the management interfaces of Cisco IOS XR Software could allow an unauthenticated, adjacent attacker to cause an IPv6 flood on the management interface network of an affected device **CVE-2021-1136, CVE-2021-1244 -** Cisco IOS XR Software for the Cisco 8000 Series Routers could allow an authenticated, local attacker to execute unsigned code during the boot process on an affected device **CVE-2021-1370** - Cisco IOS XR CLI command of running Cisco 8000 Series Routers software images could allow an authenticated, local attacker to elevate their privilege to root. To exploit this vulnerability, an attacker would need to have a valid account on an affected device **CVE-2021-1221** - User interface of Cisco Webex Software could allow an authenticated, remote attacker to inject a hyperlink into a meeting invitation email. The vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by entering a URL into a field in the user interface. **CVE-2021-1243** - Cisco IOS XR Software could allow an unauthenticated, remote attacker to allow connections that is configured to deny access to the SNMP server of an affected device. An attacker could exploit this vulnerability by connecting to an affected device using SNMP. **CVE-2021-1389** - The vulnerability is due to improper processing of IPv6 traffic that is sent through an affected device. An attacker could exploit this vulnerability by sending crafted IPv6 packets that traverse the affected device. **CVE-2021-1296, CVE-2021-1297 -** Cisco Small Business Routers could allow an unauthenticated, remote attacker to conduct directory traversal attacks and overwrite certain files that should be restricted on an affected system. An attacker could exploit these vulnerabilities by using the web-based management interface to upload a file to location on an affected device
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-rv160-260-rce-XZeFkNHf https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-xripv6-spJem78K https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ioxr-l-zNhcGCBt https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxr-pe-QpzCAePe https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-wbx-linkinj-WWZpVqu9 https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-snmp-7MKrW7Nq https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ipv6-acl-CHgdYk8j https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv160-260-filewrite-7x9mnKjn

Affected Product	**IBM WebSphere**
Severity	**Medium**
Affected Vulnerability	Directory Traversal Vulnerability (CVE-2020-4782)
Description	IBM WebSphere Application Server could allow a remote attacker to access directories on the system. An attacker could send a malicious URL request containing "dot dot" sequences to view arbitrary files on the system
Affected Products	IBM WebSphere Application Server 7.0, 8.0, 8.5, and 9.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/6412265

Affected Product	**IBM QRadar SIEM**
Severity	**Medium**
Affected Vulnerability	Denial of Service (CVE-2020-5032)
Description	IBM has released Security Updates which address denial of service vulnerability of QRadar SIEM. QRadar SIEM in some configurations may be vulnerable to a temporary denial of service attack when sent particular payloads
Affected Products	IBM QRadar SIEM 7.4.2 GA to 7.4.2 Patch 1 IBM QRadar SIEM 7.4.0 to 7.4.1 Patch 1 IBM QRadar SIEM 7.3.0 to 7.3.3 Patch 5
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/6411014

Affected Product	**Citrix**
Severity	**Low**
Affected Vulnerability	Privilege Escalation (CVE-2021-3308)
Description	An attacker could allow to execute privileged code in a guest VM to which a PCI passthrough device has been allocated can cause other VMs with PCI passthrough devices to fail to boot load or crash.
Affected Products	Citrix Hypervisor 8.2 LTSR
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.citrix.com/article/CTX291439

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.