Advisory Alert

Alert Number : AAA20210318 **Date :** March 18, 2021

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Cisco	**High**	Multiple Vulnerabilities
IBM	**High**	Multiple Vulnerabilities
Red Hat	**Medium**	Multiple Vulnerabilities

Description

Affected Product	**Cisco**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2021-1287)
Description	Certain cisco small business routers are affected by a vulnerability due to improper user input validation in the web-based management interface which allows an unauthenticated remote attacker to execute arbitrary code as the *root* user on the underlying operating system or cause the device to reload, resulting in a denial of service (DoS) condition on the affected device.
Affected Products	RV132W ADSL2+ Wireless-N VPN Routers that are running a firmware release earlier than Release 1.0.1.15 RV134W VDSL2 Wireless-AC VPN Routers that are running a firmware release earlier than Release 1.0.1.21
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-rv-132w134w-overflow-Pptt4H2p

Affected Product	**IBM**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2019-17498, CVE-2018-20843, CVE-2019-15903, CVE-2017-12652, CVE-2019-14834, CVE-2019-5482)
Description	Multiple vulnerabilities have been identified in IBM Security Access Manager and IBM Security Verify Access appliances.
Affected Products	IBM Security Access Manager version 9.0 IBM Security Verify Access version 10.0.0
Officially Acknowledged by the Vendor	yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/6430709

Affected Product	**Red Hat**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2021-20265, CVE-2019-5482)
Description	CVE-2021-20265 – The Resource Exhaustion vulnerability exists due to application does not properly control consumption of internal resources in the unix_stream_recvmsg function in the Linux kernel when a signal was pending. A local user can trigger memory exhaustion and crash the system and the availability of the system will be threatened as a result. CVE-2019-5482 - libcurl contains a heap buffer overflow in the function that receives data from a TFTP server and is triggered when a small non-default TFTP blocksize is used
Affected Products	Multiple Products
Officially Acknowledged by the Vendor	yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/security/cve/CVE-2021-20265 https://access.redhat.com/security/cve/CVE-2019-5482?extId-CarryO%20ver=true&sc_cid=701f2000001OH7JAAW

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.