Advisory Alert

Alert Number: AAA20210716 **Date:** July 16, 2021

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Microsoft	**Critical**	Elevation of privileges vulnerability
Sonicwall	**Critical**	Multiple Vulnerabilities
Cisco	**High**	Multiple Vulnerabilities
IBM	**Medium**	Information disclosure vulnerability

Description

Affected Product	Microsoft
Severity	**Critical**
Affected Vulnerability	Elevation of Privilege Vulnerability (CVE-2021-34481)
Description	Microsoft has released workarounds addressing vulnerability which exists when the Windows Print Spooler service improperly performs privileged file operations. After a successful exploitation an attacker could run arbitrary code with SYSTEM privileges and install programs, view/change/delete data or create new accounts with full user rights. Microsoft highly recommends to apply necessary workarounds at earliest to avoid issues.
Affected Products	Windows Print Spooler
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-34481

Affected Product	Sonicwall
Severity	**Critical**
Affected Vulnerability	Multiple vulnerabilities (CVE-2021-3449, CVE-2021-3450, CVE-2019-7481, CVE-2021-20016)
Description	Sonicwall has released security updates addressing multiple vulnerabilities that exists in their products including a critical risk to unpatched end-of-life SRA & SMA 8.X Remote Access Devices. The threat actors actively targeting Secure Mobile Access (SMA) 100 series and Secure Remote Access (SRA) products running unpatched and end-of-life (EOL) 8.x firmware in an imminent ransomware campaign using stolen credentials. Sonicwall highly recommends to apply necessary fixes immediately to avoid issues.
Affected Products	SMA100 10.2.0.x SonicOS(Gen7) NSa, TZ 7.0.1 Capture Client Cc 3.5 SRA and/or SMA 100 series with 8.x, 9.x and 10.x firmware
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2021-0013 https://www.sonicwall.com/support/product-notification/urgent-security-notice-critical-risk-to-unpatched-end-of-life-sra-sma-8-x-remote-access-devices/210713105333210/

Affected Product	Cisco
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2021-1422, CVE-2020-3155)
Description	Cisco has released security updates addressing multiple vulnerabilities that exists in their products. CVE-2021-1422 – An attacker could exploit this flaw by sending malicious packets over an established IPsec connection. Successful exploitation of this flaw could allow an authenticated, remote attacker or an unauthenticated attacker in a man-in-the-middle position to cause an unexpected reload of the device that results in a denial of service (DoS) condition. CVE-2020-3155 - Due to a lack of validation of the SSL server certificate received when establishing a connection to a Cisco Webex video device or a Cisco collaboration endpoint an attacker can exploit system by using man in the middle (MITM) techniques to intercept the traffic between the affected client and an endpoint, and then using a forged certificate to impersonate the endpoint. Successful exploitation could allows an unauthenticated, remote attacker to view or alter information shared on Cisco Webex video devices and Cisco collaboration. Cisco highly recommends to apply necessary security fixes to avoid issues.
Affected Products	Firepower 2100 Series Firepower NGFW Virtual Adaptive Security Virtual Appliance (ASAv) Cisco Intelligent Proximity application Cisco Jabber Cisco Webex Meetings Cisco Webex Teams Cisco Meeting App
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asa-ftd-ipsec-dos-TFKQbgWC https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-proximity-ssl-cert-gBBu3RB

Affected Product	IBM
Severity	**High**
Affected Vulnerability	Information disclosure vulnerability (CVE-2020-4980)
Description	IBM has released security updates addressing information disclosure vulnerability that exists in their products. This is due to less secure methods used in IBM QRadar SIEM for securing data at rest and in transit between hosts. IBM highly recommends to apply necessary security fixes at earliest to avoid issues.
Affected Products	IBM QRadar 7.3.0 to 7.3.3 Patch 7 IBM QRadar 7.4.0 to 7.4.3 GA
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/6472891

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.