Advisory Alert

Alert Number: AAA20210625 **Date:** June 25, 2021

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
VMware	Critical	Authentication Bypass Vulnerability
Palo Alto	Critical	Improper Authorization Vulnerability
Cisco	**High**	Multiple Vulnerabilities
Citrix	**Medium**	Allow Privileged Code
IBM	**Medium**	Multiple Vulnerabilities

Description

Affected Product	**VMware**
Severity	**Critical**
Affected Vulnerability	Authentication Bypass Vulnerability (CVE-2021-21998)
Description	VMware has released security updates addressing authentication bypass vulnerability that exists in their products. Using this flaw a malicious actor with network access to the VMware Carbon Black App Control management server might be able to obtain administrative access to the product without the need to authenticate. VMware recommends to apply necessary security fixes to avoid issues.
Affected Products	VMware Carbon Black App Control (AppC) 8.6.x, 8.5.x, 8.1.x, 8.0.x
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.vmware.com/security/advisories/VMSA-2021-0013.html

Affected Product	**Palo Alto**
Severity	**Critical**
Affected Vulnerability	Improper Authorization Vulnerability (CVE-2021-3044)
Description	An improper authorization vulnerability in Palo Alto Networks Cortex XSOAR enables a remote unauthenticated attacker with network access to the Cortex XSOAR server to perform unauthorized actions through the REST API. Palo alto recommends to apply necessary security fixes to avoid issues.
Affected Products	Cortex XSOAR 6.1.0 builds later than 1016923 and earlier than 1271064 Cortex XSOAR 6.2.0 builds earlier than 1271065
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://security.paloaltonetworks.com/CVE-2021-3044

Affected Product	**Cisco**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2020-3265, CVE-2020-3264)
Description	CVE-2020-3265 - Privilege Escalation Vulnerability in Cisco SD-WAN Solution software could allow an authenticated, local attacker to elevate privileges to root on the underlying operating system. CVE-2020-3264 - Buffer Overflow Vulnerability in Cisco SD-WAN Solution software could allow an authenticated, local attacker to cause a buffer overflow 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-sdwpresc-ySJGvE9 https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwanbo-QKcABnS2

Affected Product	**Citrix**
Severity	**Medium**
Affected Vulnerability	Allow Privileged Code (CVE-2021-3416, CVE-2021-20257)
Description	Citrix has released security updates addressing multiple vulnerabilities that exists in their products. CVE-2021-3416, CVE-2021-20257 - privileged code in a guest VM may cause the host to crash or become unresponsive.
Affected Products	Citrix Hypervisor 8.2 LTSR
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.citrix.com/article/CTX316325

Affected Product	**IBM**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2020-4885, CVE-2021-20579, CVE-2020-4945)
Description	IBM has released updates addressing multiple vulnerabilities that exists in IBM Db2. It is highly recommended to apply necessary fixes provided in official IBM website at earliest to avoid these vulnerabilities.
Affected Products	Multiple Products
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/6466363 https://www.ibm.com/support/pages/node/6466369 https://www.ibm.com/support/pages/node/6466367

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.