Advisory Alert

Alert Number: AAA20201126 **Date:** November 26, 2020

Document Classification Level : Public Circulation Permitted

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Citrix	High	Privileged code execution
cPanel	High	Multiple Vulnerabilities
Cisco	Medium	Information disclosure Vulnerability
Joomla	Low	Multiple Vulnerabilities

Description

Affected Product	Citrix
Severity	High
Affected Vulnerability	Privileged code running vulnerability
Description	Citrix has released security updates addressing vulnerability found in Citrix products which allows privileged code running in a guest VM in order to compromise the host. This will occur only on those guest VMs where the host administrator has explicitly assigned a PCI pass-through device to the guest VM.
Affected Products	Citrix Hypervisor – versions 8.1 and 8.2 LTSR Citrix XenServer – versions 7.0 and 7.1 Cumulative Update 2
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.citrix.com/article/CTX286511

Affected Product	cPanel
Severity	High
Affected Vulnerability	Multiple Vulnerabilities
Description	cPanel has released security updates addressing multiple vulnerabilities that exists in their products. The most severe vulnerability allows two factor authentication bypass using brute force techniques.
Affected Products	cPanel Versions prior to update 11.92.0.2, 11.90.0.17, 11.86.0.32
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://news.cpanel.com/cpanel-tsr-2020-0007-full-disclosure/

Affected Product	Cisco
Severity	Medium
Affected Vulnerability	Information disclosure Vulnerability (CVE-2020-3482)
Description	Cisco has released security patch updates addressing a vulnerability in the Traversal Using Relays around NAT(TURN) server component of Cisco Expressway software which could allow an unauthenticated remote attacker to bypass security controls and send network traffic to restricted destinations. The vulnerability exists due to improper validation of specific connection information by the Traversal Using Relays around NAT (TURN) server. A remote attacker can send traffic through the affected software to destinations beyond the application and gain unauthorized network access.
Affected Products	Cisco Expressway Series and Cisco TelePresence Video Communication Server (VCS) with the TURN server feature enabled and running a software release earlier than Release X12.6.3.
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-Expressway-8J3yZ7hV

Affected Product	Joomla
Severity	Low
Affected Vulnerability	Multiple Vulnerabilities
Description	Joomla has released security patch updates addressing multiple vulnerabilities that exists in their product. Joomla recommends to upgrade the existing joomla versions in to version 3.9.23 inorder to avoid issues with below mentioned versions.
Affected Products	Joomla! CMS versions 1.7.0 - 3.9.22 Joomla! CMS versions 3.9.0 - 3.9.22 Joomla! CMS versions 3.0.0 - 3.9.22 Joomla! CMS versions 2.5.0 - 3.9.22
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://developer.joomla.org/security-centre/

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.