Advisory Alert

Alert Number: AAA20210902 **Date:** September 2, 2021

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Cisco	**Critical, Medium**	Multiple Vulnerabilities
cPanel	**Medium**	Security Fixes

Description

Affected Product	Cisco
Severity	**Critical, Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2021-34746, CVE-2021-34733, CVE-2021-34732, CVE-2021-34759,CVE-2021-34765)
Description	Cisco has released Security Updates addressing multiple vulnerabilities that exists with multiple cisco products. **CVE-2021-34746** - TACACS+ authentication, authorization and accounting feature of Cisco Enterprise NFV Infrastructure Software (NFVIS) could allow an unauthenticated, remote attacker to bypass authentication and log in to an affected device as an administrator. **CVE-2021-34733** - An authorized, local attacker could get access to sensitive information stored on the underlying file system of an affected machine via the CLI of Cisco Prime Infrastructure and Cisco Evolved Programmable Network (EPN) Manager. **CVE-2021-34732, CVE-2021-34759** - An unauthenticated remote attacker could execute a cross-site scripting (XSS), Cisco Identity Services Engine (ISE) attack against a user of Cisco Prime Collaboration Provisioning's web-based administration interface. **CVE-2021-34765** - An authorized, remote attacker could use the web UI for Cisco Nexus Insights to access and download files related to the web application. Valid device credentials are required by the attacker.
Affected Products	Cisco Nexus Insights releases earlier than Release 6.0.1. Cisco Enterprise NFVIS Release 4.5.1 Cisco Prime Infrastructure releases earlier than Release 3.8 Cisco EPN Manager releases earlier than Release 5.0 Cisco ISE Software 2.2 Patch17 and earlier 2.3, Patch7 and earlier, 2.4 Patch14 and earlier, 2.6 Patch9 and earlier, 2.7 Patch4 and earlier, 3.0 Patch3 and earlierYes
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nfvis-g2DMVVh https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-prime-info-disc-nTU9FJ2 https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-prime-collab-xss-fQMDE5GO https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-xss-4HnZFewr https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-insight-infodis-2By2ZpBB

Affected Product	cPanel
Severity	**Medium**
Affected Vulnerability	Security Fixes
Description	cPanel has updated RPMs for EasyApache 4 with OpenSSL 1.1.1 and a patch for APR 1.7.0. This release addresses vulnerabilities related to CVE-2021-35940, CVE-2021-3711, and CVE-2021-3712. We already issued advisory for OpenSSL, and all APR users need to upgrade to the patched version 1.7.0.
Affected Products	APR version 1.7.0.
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://news.cpanel.com/easyapache-4-september-1-release/

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.