Advisory Alert

Alert Number: AAA20211028 **Date:** October 28, 2021

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
CPanel	**High**	Privilege Escalation
Cisco	**High, Medium**	Multiple vulnerabilities

Description

Affected Product	CPanel
Severity	**High**
Affected Vulnerability	Privilege Escalation (CVE-2021-21703)
Description	PHP FPM SAPI with main FPM daemon process running as root and child worker processes running as lower-privileged users, it is possible for the child processes to access memory shared with the main process and write to it, modifying it in a way that would cause the root process to conduct invalid memory reads and writes, which can be used to escalate privileges from local unprivileged user to the root user.
Affected Products	All versions of PHP 8.0 through 8.0.11. All versions of PHP 7.4 through 7.4.24. All versions of PHP 7.3 through 7.3.31.
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://news.cpanel.com/easyapache-4-october-27-release/

Affected Product	Cisco
Severity	**High, Medium**
Affected Vulnerability	Multiple vulnerabilities (CVE-2021-40116,CVE-2021-34783,CVE-2021-34781,CVE-2021-34752,CVE-2021-34755,CVE-2021-34756,CVE-2021-34762,CVE-2021-40117,CVE-2021-1573,CVE-2021-34704,CVE-2021-40118,CVE-2021-34792,CVE-2021-34793,CVE-2021-40114,CVE-2021-34790,CVE-2021-34791,CVE-2021-34761,CVE-2021-34753,CVE-2021-34754,CVE-2021-34763,CVE-2021-34764,CVE-2021-34750,CVE-2021-34751,CVE-2021-1444,CVE-2021-34794,CVE-2021-34787,CVE-2021-40125)
Description	Cisco has released security patch updates addressing multiple vulnerabilities that exists in multiple Cisco products. An attacker could use these vulnerabilities to gain access to systems and perform Command Injection, Denial of Service, Authorization Bypass, Directory Traversal, Cross-Site Scripting, Arbitrary File Write Vulnerability, Information Disclosure malicious activities.
Affected Products	Cisco ASA Software Cisco FTD Software Cisco FMC Software Cisco UTD Software Snort Software
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-snort-dos-RywH7ezM https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ftd-tls-decrypt-dos-BMxYjm8M https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ftd-dos-rUDseW3r https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ftd-cmdinject-FmzsLN8 https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-fmc-dir-traversal-95UyW5tk https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-dos-4ygzLKU9 https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asafdt-webvpn-dos-KSqJAKPA https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asa-ftd-dos-Unk689XY https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asa-ftd-dos-JxYWMJyL https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-snort-dos-s2R7W9UU https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-natalg-bypass-cpKGqkng https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ftd-file-write-SHVcmQVc https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ftd-enip-bypass-eFsxd8KP https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-fmc-xss-openredir-TVPMWJyg https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-fmc-infodisc-Ft2WVmNU https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-xss-webui-gQLSFyPM https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-snmpaccess-M6yOweq3 https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-rule-bypass-ejjOgQEY https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-ikev2-dos-g4cmrr7C

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.