Advisory Alert

Alert Number: AAA20210923 **Date:** September 23, 2021

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Cisco	**Critical**	Multiple Vulnerabilities
cPanel	**Medium**	Multiple Vulnerabilities

Description

Affected Product	**Cisco**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2021-34727, CVE-2021-34770, CVE-2021-1619, CVE-2021-34699, CVE-2021-1624, CVE-2021-1621, CVE-2021-1615, CVE-2021-1620, CVE-2021-34705, CVE-2021-34767, CVE-2021-1611, CVE-2021-1565, CVE-2021-34768, CVE-2021-34769, CVE-2021-1419, CVE-2021-1623, CVE-2021-1622, CVE-2021-34740, CVE-2021-34697, CVE-2021-1625, CVE-2021-34725, CVE-2021-34726, CVE-2021-34712, CVE-2021-1589, CVE-2021-1612, CVE-2021-1546, CVE-2021-34703, CVE-2021-34729, CVE-2021-34724, CVE-2021-34723, CVE-2021-1616, CVE-2021-34714, CVE-2021-34696)
Description	Cisco has released Security Updates addressing multiple vulnerabilities that exist with various cisco products such as Buffer Overflow Vulnerability, Remote Code Execution Vulnerability, Authentication Bypass Vulnerability, Denial of Service Vulnerability, Command Injection Vulnerability, Privilege Escalation Vulnerability, Password Exposure Vulnerability, Arbitrary File Overwrite Vulnerability. It is highly recommended to apply necessary fixes provided on the official Cisco website at the earliest to avoid these security issues, and all Cisco users are encouraged to upgrade to the latest versions.
Affected Products	Cisco ASR 900 and ASR 920 Series Cisco IOS XE Software Cisco IOS XE SD-WAN Cisco SD-WAN vManage Cisco Access Points Cisco Embedded Wireless Controller Software Cisco IOS Software
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://tools.cisco.com/security/center/publicationListing.x

Affected Product	**EasyApache 4**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2021-22945, CVE-2021-22946, CVE-2021-22947, CVE-2021-40438, CVE-2021-39275, CVE-2021-36160, CVE-2021-34798, CVE-2021-33193)
Description	cPanel has released an update for EasyApache 4, including new packages for EasyApache 4 with Apache 2.4.49 and libcurl 7.79.0. Also, this update addressing multiple vulnerabilities that exists in their products. **CVE-2021-40438 -** A specially constructed request uri-path can cause mod_proxy to send the request to a remote user-selected origin server. **CVE-2021-39275 -** When provided malicious data, ap_escape_quotes() may write past the end of a buffer. Third-party / external modules may transmit untrusted data to these functions, although no included modules do. **CVE-2021-36160 -** mod_proxy_uwsgi can crash (DoS) if a carefully designed request uri-path reads beyond the allotted memory. **CVE-2021-34798 -** Malformed requests may cause the server to dereference a NULL pointer. **CVE-2021-33193 -** A contrived HTTP/2 method will evade validation and be transmitted by mod_proxy, potentially resulting in request splitting or cache poisoning. **CVE-2021-22945 -** When transmitting data to an MQTT server, libcurl may maintain an erroneous pointer to a previously freed memory area and both use and free it in a future call to submit data. **CVE-2021-22946 -** When communicating with an IMAP, POP3, or FTP server, a user can tell curl to need a successful upgrade to TLS (--ssl-reqd on the command line or CURLOPT_USE_SSL set to CURLUSESSL_CONTROL or CURLUSESSL_ALL with libcurl). If the server sends a well-crafted but completely legitimate response, this requirement may be bypassed. **CVE-2021-22947 -** The server can still respond and send back numerous responses before the TLS upgrade when curl connects to an IMAP, POP3, SMTP, or FTP server to exchange data securely using STARTTLS to upgrade the connection to TLS level. Curl caches such many "pipelined" responses. Instead of flushing the in-queue of cached replies, curl would use and trust the responses it received before the TLS handshake as though they were authenticated.
Affected Products	All versions of Apache through 2.4.48. All versions of libcurl through 7.78.0.
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://news.cpanel.com/easyapache-4-september-22-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.