



Advisory Alert

Alert Number: AAA20210730

Date: July 30, 2021

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
IBM	Medium	Privilege Escalation
cPanel	Medium	Security Patch updates

Description

Affected Product	IBM
Severity	Medium
Affected Vulnerability	Privilege Escalation (CVE-2021-29736)
Description	WebSphere Application Server is vulnerable to a privilege escalation vulnerability it could allow a remote user to gain access to the system.
Affected Products	WebSphere Application Server 9.0 WebSphere Application Server 8.5 WebSphere Application Server 8.0 WebSphere Application Server 7.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/6476678

Affected Product	cPanel
Severity	Medium
Affected Vulnerability	Security Patch updates (CVE-2021-22922, CVE-2021-22923, CVE-2021-22924, CVE-2021-22925, CVE-2021-22926)
Description	cPanel has released updates addressing security fixes that exist in EasyApache 4 with libcurl. It is highly recommended to apply necessary fixes provided on the official cPanel website at the earliest to avoid these security issues and all cPanel users are encouraged to upgrade latest versions
Affected Products	All versions of libcurl through 7.77.0.
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://news.cpanel.com/easyapache-4-july-28-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.