Advisory Alert

Alert Number: **AAA20250612** **Date:** **June 12, 2025**

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
IBM	**Critical**	HTTP Request/Response Smuggling Vulnerability
IBM	**High, Medium, Low**	Multiple Vulnerabilities
cPanel	**Low**	Security Update

Description

Affected Product	**IBM**
Severity	**Critical**
Affected Vulnerability	HTTP Request/Response Smuggling Vulnerability (CVE-2025-43859)
Description	IBM has released security updates addressing an HTTP request/response smuggling vulnerability that exists in their products. **CVE-2025-43859** - h11 is a Python implementation of HTTP/1.1. Prior to version 0.16.0, a leniency in h11's parsing of line terminators in chunked-coding message bodies can lead to request smuggling vulnerabilities under certain conditions. This issue has been patched in version 0.16.0. Since exploitation requires the combination of buggy h11 with a buggy (reverse) proxy, fixing either component is sufficient to mitigate this issue. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	IBM Security QRadar EDR Versions - 3.12
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7236354

Affected Product	**IBM**
Severity	**High, Medium, Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-53382, CVE-2025-27789, CVE-2025-30204, CVE-2024-51744, CVE-2024-12905, CVE-2025-27516, CVE-2025-47935, CVE-2025-47944, CVE-2024-6827, CVE-2024-49350, CVE-2024-7254)
Description	IBM has released security updates addressing multiple vulnerabilities that exists in their products. These vulnerabilities could be exploited by malicious users to cause buffer overflow, information disclosure, improper input validation and code injection. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	IBM Security QRadar EDR Versions - 3.12 IBM Db2 Server versions 11.1.0 - 11.1.4.7, 11.5.0 - 11.5.9 and 12.1.0 - 12.1.1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.ibm.com/support/pages/node/7236354 • https://www.ibm.com/support/pages/node/7235069 • https://www.ibm.com/support/pages/node/7235067

Affected Product	**cPanel**
Severity	Low
Affected Vulnerability	Security Update (CVE-2025-5399)
Description	cPanel has released security updates addressing a vulnerability that exists in their products. **CVE-2025-5399** - Due to a mistake in libcurl's WebSocket code, a malicious server can send a particularly crafted packet which makes libcurl get trapped in an endless busy-loop. There is no other way for the application to escape or exit this loop other than killing the thread/process. This might be used to DoS libcurl-using application. cPanel advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	All cPanel versions of libcurl through 8.14.0.
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://news.cpanel.com/easyapache4-v25-19-maintenance-and-security-release/

Disclaimer

The information provided are gathered from official service provider's websites and portals. FinCSIRT strongly recommends members to apply security fixes as per the given guidelines, following the organization's patch and change management procedures to protect systems from potential threats.