Advisory Alert

Alert Number: AAA20251209 **Date:** December 9, 2025

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
React	**Critical**	Unauthenticated Remote Code Execution Vulnerability
Next.js	**Critical**	Unauthenticated Remote Code Execution Vulnerability
F5	**High**	Security Update
IBM	**Medium**	Improper User-Supplied Input Validation Vulnerability
Citrix	**Medium**	Security Update
Red Hat	**Medium**	Multiple Vulnerabilities
cPanel	**Medium**, **Low**	Multiple Vulnerabilities

Description

Affected Product	**React**
Severity	**Critical**
Affected Vulnerability	Unauthenticated Remote Code Execution Vulnerability (CVE-2025-55182)
Description	Meta has released security updates addressing an Unauthenticated Remote Code Execution Vulnerability that exists in React Server Components. **CVE-2025-55182** - React Server Functions allow a client to call a function on a server. React provides integration points and tools that frameworks and bundlers use to help React code run on both the client and the server. React translates requests on the client into HTTP requests which are forwarded to a server. On the server, React translates the HTTP request into a function call and returns the needed data to the client. An unauthenticated attacker could craft a malicious HTTP request to any Server Function endpoint that, when deserialized by React, achieves remote code execution on the server. Meta advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	React versions 19.0, 19.1.0, 19.1.1, and 19.2.0 with below packages: • react-server-dom-webpack • react-server-dom-parcel • react-server-dom-turbopack Note - Even if the app does not implement any React Server Function endpoints it may still be vulnerable if the app supports React Server Components.
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://react.dev/blog/2025/12/03/critical-security-vulnerability-in-react-server-components

Affected Product	**Next.js**
Severity	**Critical**
Affected Vulnerability	Unauthenticated Remote Code Execution Vulnerability (CVE-2025-66478)
Description	Vercel has released security updates addressing an Unauthenticated Remote Code Execution Vulnerability that exist in in the React Server Components (RSC) protocol which affects Next.js. **CVE-2025-66478** - The vulnerable RSC protocol allowed untrusted inputs to influence server-side execution behavior. Under specific conditions, an attacker could craft requests that trigger unintended server execution paths. This can result in remote code execution in unpatched environments. Vercel advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Applications using React Server Components with the App Router are affected when running • Next.js 15.x • Next.js 16.x • Next.js 14.3.0-canary.77 and later canary releases
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://nextjs.org/blog/CVE-2025-66478

Affected Product	**F5**
Severity	**High**
Affected Vulnerability	Security Update (CVE-2020-7595)
Description	F5 has released security updates addressing a vulnerability that exists in libxml2 which affects F5OS. An attacker could exploit this vulnerability to cause the application to enter into an infinite loop resulting in a denial of service (DoS). F5 advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	F5OS versions 1.1.0 - 1.2.2
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://my.f5.com/manage/s/article/K04460334

Affected Product	**IBM**
Severity	**Medium**
Affected Vulnerability	Improper User-Supplied Input Validation Vulnerability (CVE-2025-12635)
Description	IBM has released security updates addressing an Improper User-Supplied Input Validation Vulnerability that exists in IBM WebSphere Application Server and WebSphere Application Server Liberty. **CVE-2025-12635** - IBM WebSphere Application Server and IBM WebSphere Application Server Liberty are affected by cross-site scripting due to improper validation of user-supplied input. An attacker could exploit this vulnerability by using a specially crafted URL to redirect the user to a malicious site. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	IBM WebSphere Application Server versions 9.0 and 8.5 IBM WebSphere Application Server – Liberty versions 17.0.0.3 - 25.0.0.12
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7254078

Affected Product	**Citrix**
Severity	**Medium**
Affected Vulnerability	Security Update (CVE-2025-62626)
Description	Citrix has released security updates addressing a vulnerability that exists in a third party product which affects XenServer. A hardware issue has been identified in AMD Zen 5 CPU devices that may cause those CPUs to return a value of zero more frequently than statistically expected when asked to generate a random value. This may compromise e.g. cryptographic keys that are generated by software that relies on the randomness of these values. Citrix advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	XenServer 8.4.
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.citrix.com/support-home/kbsearch/article?articleNumber=CTX695797&articleURL=XenServer_Security_Update_for_CVE_2025_62626

Affected Product	**Red Hat**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-38737, CVE-2025-39925, CVE-2025-39979, CVE-2025-39981, CVE-2025-39982, CVE-2025-39983, CVE-2025-40047, CVE-2025-40058, CVE-2025-40185)
Description	Red Hat has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to compromise the affected system. Red Hat advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Red Hat Enterprise Linux for x86_64 10 x86_64 Red Hat Enterprise Linux for IBM z Systems 10 s390x Red Hat Enterprise Linux for Power, little endian 10 ppc64le Red Hat Enterprise Linux for ARM 64 10 aarch64 Red Hat CodeReady Linux Builder for x86_64 10 x86_64 Red Hat CodeReady Linux Builder for Power, little endian 10 ppc64le Red Hat CodeReady Linux Builder for ARM 64 10 aarch64 Red Hat CodeReady Linux Builder for IBM z Systems 10 s390x
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2025:22854

Affected Product	**cPanel**
Severity	**Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-55753, CVE-2025-58098, CVE-2025-59775, CVE-2025-65082, CVE-2025-66200)
Description	cPanel has released security updates addressing multiple vulnerabilities that exist in EasyApache 4. These vulnerabilities could be exploited by malicious users to cause Command Execution, Server-side Request Forgery, bypass security restrictions. cPanel advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	ea-apache24 v2.4.65
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://docs.cpanel.net/changelogs/easyapache-4-change-log-25/

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.