Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

VULNERABILITY REPORT

XRP at Risk: Malicious xrpl.js Update Steals Wallet Keys

Date of Publication	Admiralty Code	TA Number
April 25, 2025	A1	TA2025125

Summary

First Seen: April 2025
Affected Products: xrpl.js
Impact: A critical supply chain vulnerability tracked as CVE-2025-32965 has been uncovered in the popular JavaScript library xrpl.js, used to interact with the XRP Ledger. Malicious versions were uploaded to NPM and designed to exfiltrate wallet seeds and private keys to an attacker-controlled server, enabling theft of users' funds. These versions did not match official GitHub releases raising red flags and contained hidden backdoors inserted through both TypeScript and compiled JavaScript code.

CVE

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2025-32965	xrpl.js Supply Chain Vulnerability	xrpl.js	✗	✗	✓

Vulnerability Details

#1 CVE-2025-32965 is a supply chain vulnerability affecting the widely used JavaScript library xrpl.js, which facilitates interaction with the XRP Ledger. This flaw stems from malicious versions of the library starting with version 4.2.1 uploaded to the NPM registry beginning April 21, 2025. These tampered releases contained hidden code designed to silently exfiltrate XRP wallet seeds and private keys to an attacker-controlled domain whenever a Wallet object was initialized, putting users' funds at serious risk of theft.

#2 Notably, these malicious versions did not align with the official GitHub releases maintained by XRPLF, raising red flags. The attacker carefully altered both the JavaScript and TypeScript codebases to conceal their backdoor. The version 4.2.2 was the first to introduce malicious payloads, followed by further obfuscated versions like 4.2.3 and 4.2.4, which embedded the backdoor more deeply.

#3 The attack complexity is low, making the vulnerability significantly more dangerous. The flaw is remotely exploitable without any user interaction. This incident highlights the growing threat of supply chain attacks, particularly in widely used open-source libraries. Developers using xrpl.js are urged to verify their dependencies, downgrade to a safe version if impacted, and rotate any exposed wallet credentials immediately.

Vulnerability

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2025-32965	xrpl.js Versions 4.2.1, 4.2.2, 4.2.3, 4.2.4 and Version 2.14.2	cpe:2.3:a:xrpl.js:xrpl.js:*:*:*:*:*:*:*:*	CWE-506

Recommendations

Immediately Audit Your Codebase: Take a moment to review your projects and apps to see if they use the affected xrpl.js versions especially 4.2.1 through 4.2.4. If any of those versions are in use, remove them right away and switch to the latest safe release from the official XRPL GitHub repository.

Rotate Compromised Wallet Credentials: If you've used any of the affected xrpl.js versions in your projects, it's safest to assume your wallet seeds or private keys may have been exposed. Act quickly generate new keys, move your funds to secure wallets, and retire any wallets that may have been compromised.

Use Trusted and Verified Sources: Don't rely only on NPM when pulling in critical libraries always double-check that the package matches the official GitHub release or trusted vendor source. When possible, stick to libraries that support package signing or reproducible builds, so you know exactly what you're installing.

Vulnerability Management: This involves regularly assessing and updating software to address known vulnerabilities. Maintain an inventory of software versions and security patches, and evaluate the security practices of third-party vendors, especially for critical applications and services.

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	TA0001 Initial Access	TA0002 Execution	TA0005 Defense Evasion
TA0010 Exfiltration	T1588 Obtain Capabilities	T1588.006 Vulnerabilities	T1059 Command and Scripting Interpreter
T1059.007 JavaScript	T1190 Exploit Public-Facing Application	T1656 Impersonation	T1195 Supply Chain Compromise

Indicators of Compromise (IOCs)

TYPE	VALUE
Domain	0x9c[.]xyz

Patch Details

The xrpl team has released patched versions 4.2.5 and 2.14.3 to replace the compromised xrpl.js packages and secure against CVE-2025-32965.

Link: https://github.com/XRPLF/xrpl.js/releases

References

https://github.com/XRPLF/xrpl.js/security/advisories/GHSA-33qr-m49q-rxfx

https://www.aikido.dev/blog/xrp-supplychain-attack-official-npm-package-infected-with-crypto-stealing-backdoor

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.

REPORT GENERATED ON

April 23, 2025 • 6:30 AM

More at www.hivepro.com