FORTINET

OUTBREAK ALERTS

VM2 Sandbox Escape Vulnerability

Critical flaws in a widely used JavaScript sandbox library

https://github.com/patriksimek/vm2/security/advisories/GHSA-ch3r-j5x3-6q2m
CVEs: CVE-2022-36067, CVE-2023-29017, CVE-2023-29199, CVE-2023-30547

vm2 is a sandbox solution that can run untrusted code with whitelisted Node's built-in modules. Exploiting the flaws, threat actors can bypass the sandbox protections to gain remote code execution rights on the host running the sandbox.

Background

According to NPM, vm2 package has over 3,500,000+ weekly downloads and because of its wide usage by other applications, it ultimately puts them at risk of exploitation. For example, according to a research, Backstage, an open platform for building developer portals uses vm2 and the research shows how it can be exploited leveraging the vm2 sandbox escape vulnerability.
https://www.oxeye.io/blog/remote-code-execution-in-spotifys-backstage

Backstage platform is used by various organizations such as Netflix, Splunk, Spotify, Palo Alto Networks, Wealthsimple, etc.
https://github.com/backstage/backstage/blob/master/ADOPTERS.md

Announced

Aug 28, 2022: GitHub issued CVE-2022-36067 and released a public advisory.
https://github.com/patriksimek/vm2/security/advisories/GHSA-mrgp-mrhc-5jrq

Latest Developments

Oct 10, 2022: The vulnerability (CVE-2022-36067) was disclosed and the issue was patched in version 3.9.11.
https://www.oxeye.io/blog/vm2-sandbreak-vulnerability-cve-2022-36067

April 6, 2023: CVE-2023-29017 was discovered in version <= 3.9.14 and published with proof-of-concept (PoC) and vendor has provided the fix in vm2 version 3.9.15.
https://github.com/patriksimek/vm2/security/advisories/GHSA-7jxr-cg7f-gpgv
https://github.com/patriksimek/vm2/releases/tag/3.9.15

April 14, 2023: CVE-2023-29199 was discovered and patched in the version 3.9.16 of vm2.
https://github.com/advisories/GHSA-xj72-wvfv-8985

April 17, 2023: CVE-2023-30547 was discovered and advisory released. The fix was provided in the version 3.9.17 of vm2.
https://github.com/patriksimek/vm2/security/advisories/GHSA-ch3r-j5x3-6q2m

FortiGuard Labs has updated the IPS signature (ID:52237) to detect and block attacks leveraging the vm2 sandbox vulnerabilities (CVE-2022-36067, CVE-2023-29017, CVE-2023-29199, CVE-2023-30547). Users are recommended to apply patch as per vendor's instructions.

PROTECT

Countermeasures across the security fabric for protecting assets, data and network from cybersecurity events:

- Reconnaissance
- Weaponization
- Delivery
- **Exploitation**

IPS

Detects and blocks attacks leveraging vm2 Sandbox Vulnerabilities

FortiGate	FortiSASE	FortiNDR	FortiADC	FortiProxy
DB 23.537	*DB 23.537*	*DB 23.537*	*DB 23.537*	*DB 23.537*

Web App Security

Detects and blocks attacks leveraging vm2 Sandbox Vulnerabilities

FortiWeb	FortiADC
DB 0.00331	*DB 1.00042*

- Installation
- C2
- Action

DETECT

Find and correlate important information to identify an outbreak, the following updates are available to raise alert and generate reports:

Outbreak Detection

FortiAnalyzer
DB 1.00076

Threat Hunting

FortiAnalyzer	FortiSIEM
v7.0+	*v6.6.0+*

Content Update

FortiSIEM
DB 308

RESPOND

Develop containment techniques to mitigate impacts of security events:

Automated Response

Services that can automatically respond to this outbreak.

FortiXDR

Assisted Response Services

Experts to assist you with analysis, containment and response activities.

Incident Response	FortiRecon: ACI

RECOVER

Improve security posture and processes by implementing security awareness and training, in preparation for (and recovery from) security incidents:

InfoSec Services

Security readiness and awareness training for SOC teams, InfoSec and general employees.

Response Readiness

IDENTIFY

Identify processes and assets that need protection:

Attack Surface Monitoring (Inside & Outside)

Security reconnaissance and penetration testing services, covering both internal & external attack vectors, including those introduced internally via software supply chain.

Security Rating	FortiRecon: EASM	FortiDevSec

Additional Resources

FortiGuard Threat Signal	https://www.fortiguard.com/threat-signal-report/5132
Oxeye Research- vm2	https://www.oxeye.io/blog/vm2-sandbreak-vulnerability-cve-2022-36067
Oxeye Research- Backstage	https://www.oxeye.io/blog/remote-code-execution-in-spotifys-backstage
Bleeping Computer	https://www.bleepingcomputer.com/news/security/critical-vm2-flaw-lets-attackers-run-code-outside-the-sandbox/
Dark Reading	https://www.darkreading.com/application-security/critical-open-source-vm2-sandbox-escape-bug-affects-millions
SecurityWeek	https://www.securityweek.com/organizations-warned-critical-vulnerability-backstage-developer-portal-platform
The Hacker News	https://thehackernews.com/2023/04/researchers-discover-critical-remote.html
The Hacker News	https://thehackernews.com/2023/04/critical-flaws-in-vm2-javascript.html?m=1

Learn more about FortiGuard Outbreak Alerts