FORTINET

FortiGuard Labs Outbreak Alerts

React2Shell Remote Code Execution

Critical Unauthenticated RCE in React Server Components Actively Exploited in the Wild

https://react.dev/blog/2025/12/03/critical-security-vulnerability-in-react-server-components

CVEs: CVE-2025-55182,CVE-2025-66478

React2Shell is a critical unauthenticated remote code execution (RCE) vulnerability affecting React Server Components (RSC) and frameworks that implement the Flight protocol, including specific vulnerable versions of Next.js. A remote attacker can craft a malicious RSC request that triggers server-side deserialization, leading to arbitrary code execution without authentication or user interaction.

Background

Due to the widespread use of React and Next.js in production environments, organizations are strongly urged to apply patches immediately, enforce WAF protections on RSC/Flight endpoints, and conduct proactive threat hunting. CISA has added CVE-2025-55182 to the Known Exploited Vulnerabilities (KEV) catalog following confirmed evidence of active exploitation. AWS Security has also reported exploitation activity originating from infrastructure historically linked to China state-nexus threat actors.

Successful exploitation can lead to:
- Full server compromise, including deployment of persistent backdoors
- Credential harvesting and access to sensitive application data
- Execution of arbitrary Node.js commands on the affected server
- Lateral movement across connected systems and cloud environments

Latest Developments

Organizations should review the vendor advisories for complete version details, mitigation steps, and updated guidance. FortiGuard customers are protected by multiple layers of defense against these exploits. Refer to the Solutions tab for for information.

- December 12, 2025: Multiple Threat Actors Exploit React2Shell: Google Threat Intelligence Group https://cloud.google.com/blog/topics/threat-intelligence/threat-actors-exploit-react2shell-cve-2025-55182/
- December 05, 2025: CISA has added CVE-2025-55182 to the Known Exploited Vulnerabilities (KEV) catalog following evidence of active exploitation.
- December 05, 2025: FortiGuard Labs released a Threat Signal for React2Shell Remote Code Execution (RCE) Vulnerability. https://www.fortiguard.com/threat-signal-report/6281/react2shell-remote-code-execution-rce-vulnerability
- December 04, 2025: Lacework FortiCNAPP Protection update and response added for React & NextJS Remote Code Execution Vulnerability. https://community.fortinet.com/t5/Lacework/Technical-Tip-How-does-Lacework-FortiCNAPP-Protect-from-CVE-2025/ta-p/421658
- December 04, 2025: AWS Security has observed exploitation activity originating from infrastructure historically linked to China-nexus threat actors, noting rapid mass exploitation of vulnerable internet-facing RSC/Next.js deployments.
- December 03, 2025: Security Advisory released by Next.js and fix was published to npm and the publicly disclosed as CVE-2025-55182. https://nextjs.org/blog/CVE-2025-66478
- November 30, 2025: Meta security researchers confirmed and began working with the React team on a fix.
- November 29, 2025: Lachlan Davidson reported the security vulnerability via Meta Bug Bounty. https://react.dev/blog/2025/12/03/critical-security-vulnerability-in-react-server-components

PROTECT

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

Lure

FortiDeceptor — *DB 20260211*

Decoy VM

FortiDeceptor — *DB 20260211*

AV

Detects known malware related to the Outbreak

FortiADC — *DB 93.06352*
FortiCASB — *DB 93.06352*
FortiCWP — *DB 93.06352*
FortiClient — *DB 93.06352*
FortiGate — *DB 93.06352*
FortiMail — *DB 93.06352*
FortiProxy — *DB 93.06352*
FortiSASE — *DB 93.06352*
FortiWeb — *DB 93.06352*

AV (Pre-filter)

Detects known malware related to the Outbreak

FortiEDR — *DB 93.06352*
FortiNDR — *DB 93.06352*
FortiSandbox — *DB 93.06352*

IPS

Detects and blocks attack attempts leveraging the vulnerability

FortiADC — *DB 35.129*
FortiGate — *DB 35.129*
FortiNDR — *DB 35.129*
FortiProxy — *DB 35.129*
FortiSASE — *DB 35.129*

Web App Security

Detects and blocks attack attempts leveraging the vulnerability

FortiADC — *DB 1.00068*
FortiWeb — *DB 0.00415*

Web & DNS Filter

FortiGate

DETECT

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

IOC

FortiAnalyzer
FortiSOCaaS
FortiSIEM
FortiSOAR

Outbreak Detection

FortiAnalyzer — *DB 2.00087*
FortiNDR Cloud
FortiSIEM
FortiSOAR

Cloud Threat Detection

Lacework CNAPP

RESPOND

Develop containment techniques to mitigate impacts of security events:

Automated Response

Services that can automaticlly respond to this outbreak.

FortiXDR

Assisted Response Services

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

Incident Response

RECOVER

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

NOC/SOC Training

Train your network and security professionals and optimize your incident response to stay on top of the cyberattacks.

NSE Training
Response Readiness

End-User Training

Raise security awareness to your employees that are continuously being targeted by phishing, drive-by download and other forms of cyberattacks.

Security Awareness & Training

IDENTIFY

Identify processes and assets that need protection:

Attack Surface Hardening

Check Security Fabric devices to build actionable configuration recommendations and key indicators.

Security Rating

Additional Resources

React Blog	https://react.dev/blog/2025/12/03/critical-security-vulnerability-in-react-server-components
Google Cloud Guidance	https://cloud.google.com/blog/products/identity-security/responding-to-cve-2025-55182
Next.js Advisory	https://nextjs.org/blog/CVE-2025-66478
AWS Security Blog	https://aws.amazon.com/blogs/security/china-nexus-cyber-threat-groups-rapidly-exploit-react2shell-vulnerability-cve-2025-55182/

Learn more about FortiGuard Outbreak Alerts

FortiGuard Labs

FORTINET