OUTBREAK ALERTS



WooCommerce Payments Improper Authentication Vulnerability **Actively exploited to takeover WordPress websites**

https://developer.woocommerce.com/2023/03/23/critical-vulnerability-detected-in-woocommerce-payments-what-you-need-to-know/

CVEs: CVE-2023-28121

An authentication bypass vulnerability affecting the WooCommerce Payments plugin version 4.8.0 through 5.6.1. Successful exploitation of the

vulnerability could allow an unauthorized attacker to gain admin privileges on the WordPress websites potentially leading to the site takeover, impersonate arbitrary users, including an administrator.

Background

popular e-commerce payment plugin for WordPress sites designed for small to large-sized online merchants. According to Woo, the plugin has over 600,000 active installations. July 17, 2023: Cybersecurity Researchers at wordfence released a detailed analysis on campaign targeting

WooCommerce is a open-source commerce solution built on WordPress and WooCommerce Payments is a

wordpress sites. https://www.wordfence.com/blog/2023/07/massive-targeted-exploit-campaign-against-woocommerce-payments-underway/

July 18, 2023: FortiGuard released a Threat signal.

July 24, 2023: FortiGuard Labs has released an IPS signature to detect and block any attack attempts relating to

https://www.fortiguard.com/threat-signal-report/5223/

To mitigate any further risks update the WooCommerce Payments plugin to version 5.6.2 and later.

DB 91.0546

DB 91.0546

the vulnerability (CVE-2023-28121) and has blocked attack attempts on upto more than 4000+ unique IPS

PROTECT

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

events: Reconnaissance

devices.

Weaponization

Delivery

AV

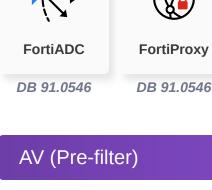
Detects and blocks malware exploiting WooCommerce Payments vulnerability (CVE-2023-28121)

DB 91.0546

FortiGate FortiWeb FortiClient FortiSASE FortiMail FortiCASB

DB 91.0546

DB 91.0546



FortiEDR FortiSandbox

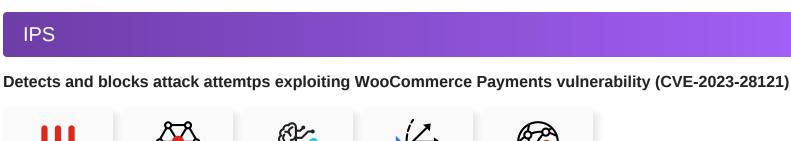
DB 91.0546 DB 91.0546



IPS

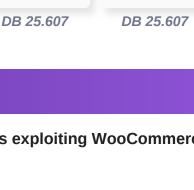
FortiGate

DB 25.607



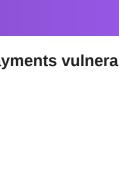


FortiNDR



FortiADC

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



FortiProxy

DB 25.607



DETECT



FortiAnalyzer

alert and generate reports:



FortiSIEM

DB 319



FortiXDR

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

(and recovery from) security incidents:



Readiness

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

Business Reputation

FortiDAST

FortiRecon: **EASM**



Additional Resources

bleeping Computer

Hacker News

https://www.bleepingcomputer.com/news/security/hackers-exploiting-critical-wordpress-woocommerce-payments-

https://thehackernews.com/2023/07/cybercriminals-exploiting-woocommerce.html

Learn more about FortiGuard Outbreak Alerts

bug/#google_vignette

F

FortiCWP

DB 91.0546

Announced

Latest Developments























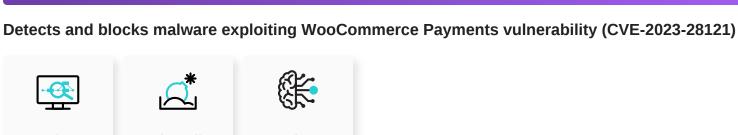










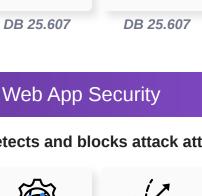


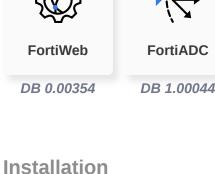


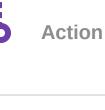


DB 91.0546









C2





Threat Hunting



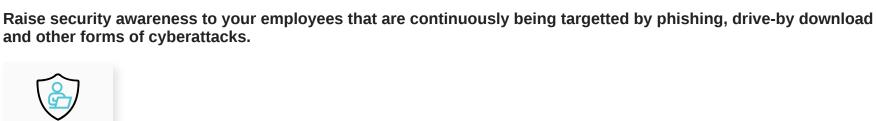


FortiRecon: Incident Response

RECOVER

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

Improve security posture and processes by implementing security awareness and training, in preparation for



Awareness & **Training**

End-User Training





Security

Rating

