

## 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	WooCommerce is a open-source commerce solution built on WordPress and WooCommerce Payments is a 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.
Latest Developments	<p>To mitigate any further risks update the WooCommerce Payments plugin to version 5.6.2 and later.</p> <p>July 24, 2023: FortiGuard Labs has released an IPS signature to detect and block any attack attempts relating to the vulnerability (CVE-2023-28121) and has blocked attack attempts on upto more than 4000+ unique IPS devices.</p> <p>July 18, 2023: FortiGuard released a Threat signal.  <a href="https://www.fortiguard.com/threat-signal-report/5223/">https://www.fortiguard.com/threat-signal-report/5223/</a></p> <p>July 17, 2023: Cybersecurity Researchers at wordfence released a detailed analysis on campaign targeting wordpress sites.  <a href="https://www.wordfence.com/blog/2023/07/massive-targeted-exploit-campaign-against-woocommerce-payments-underway/">https://www.wordfence.com/blog/2023/07/massive-targeted-exploit-campaign-against-woocommerce-payments-underway/</a></p>

## PROTECT

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




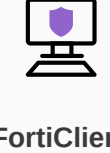





### Reconnaissance

### Weaponization

### Delivery

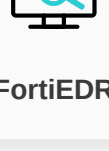
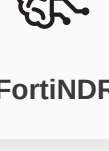
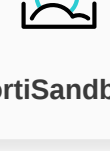
#### AV

Detects known malware related to the Outbreak

 FortiADC DB 91.0546	 FortiCASB DB 91.0546	 FortiCWP DB 91.0546	 FortiClient DB 91.0546	 FortiGate DB 91.0546	 FortiMail DB 91.0546	 FortiProxy DB 91.0546
 FortiSASE DB 91.0546	 FortiWeb DB 91.0546					

#### AV (Pre-filter)

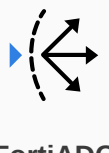




Detects known malware related to the Outbreak

 FortiEDR DB 91.0546	 FortiNDR	 FortiSandbox DB 91.0546
---	---	---

### Exploitation

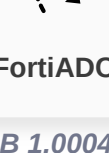
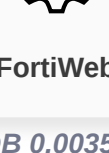
#### IPS

Detects and blocks attack attempts leveraging the vulnerability

 FortiADC DB 25.607	 FortiGate DB 25.607	 FortiNDR DB 25.607	 FortiProxy DB 25.607	 FortiSASE DB 25.607
--	---	--	--	---

#### Web App Security

Detects and blocks attack attempts leveraging the vulnerability

 FortiADC DB 1.00044	 FortiWeb DB 0.00354
---	---

### Installation




### C2

### Action


## 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
--	--	--

#### Outbreak Detection

 FortiAnalyzer DB 2.00013
--

#### Threat Hunting


 FortiAnalyzer v6.4+
---

## 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	 FortiRecon: ACI
--	--

## 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
--

#### Business Reputation

Know attackers next move to protect against your business branding.

 FortiRecon: EASM
---

## Additional Resources

Hacker News	<a href="https://thehackernews.com/2023/07/cybercriminals-exploiting-woocommerce.html">https://thehackernews.com/2023/07/cybercriminals-exploiting-woocommerce.html</a>
bleeping Computer	<a href="https://www.bleepingcomputer.com/news/security/hackers-exploiting-critical-wordpress-woocommerce-payments-bug/#google_vignette">https://www.bleepingcomputer.com/news/security/hackers-exploiting-critical-wordpress-woocommerce-payments-bug/#google_vignette</a>
About FortiGuard Outbreak Alerts	<a href="https://community.fortinet.com/t5/FortiGuard/FortiGuard-Outbreak-Alert-Version-4-0-nbsp/ta-p/315029">https://community.fortinet.com/t5/FortiGuard/FortiGuard-Outbreak-Alert-Version-4-0-nbsp/ta-p/315029</a>

Learn more about [FortiGuard Outbreak Alerts](#)