FORTINET

OUTBREAK ALERTS

WordPress WPGateway Plugin Vulnerability

Zero-day in WPGateway WordPress plugin actively being exploited

https://www.wordfence.com/blog/2022/09/psa-zero-day-vulnerability-in-wpgateway-actively-exploited-in-the-wild/

CVEs: CVE-2022-3180

The WPGateway plugin vulnerability can allow an unauthenticated remote attacker to add a malicious user with admin privileges and completely take over the WordPress sites.

Background

The WPGateway is a premium plugin which is offered as a part of WPGateway cloud service that lets users setup and manage WordPress sites from a single dashboard. On September 8, 2022, Wordfence became aware of this actively exploited zero-day vulnerability being targeted in the wild.

Announced

September 9, 2022: Wordfence disclosed the vulnerability to the WPGateway plugin vendor.

Latest Developments

September 13, 2022: Wordfence posted a blog about the vulnerability and released a public service announcement stating over 280 thousand WordPress sites have been attacked. If using WordPress for websites, FortiGuard Labs recommends having a WAF in place, such as FortiWeb Cloud, a cloud native SaaS based web application firewall (WAF) that protects web applications & APIs from zero-day attacks, other application layer attacks and requires no changes to your sites.

FortiWeb Cloud WAF-as-a-Service:
https://www.fortiweb-cloud.com

PROTECT

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

Reconnaissance

Decoy VM

Detects malicious activities related to WPGateway plugin (CVE-2022-3180

FortiDeceptor
v3.3+

Weaponization

Delivery

Exploitation

IPS

Blocks attack attempts related to WPgateway plugin (CVE-2022-3180)

FortiGate *DB 22.395*
FortiSASE *DB 22.395*
FortiNDR *DB 22.395*
FortiADC *DB 22.395*
FortiProxy *DB 22.395*

Web App Security

Blocks attack attempts related to WPgateway plugin (CVE-2022-3180)

FortiWeb *DB 0.00329*

Installation

Post-execution

Detects suspicious behavior related to malicious admin user creation exploiting WPGateway Vulnerability (CVE-2022-3180)

FortiEDR *v5.0+*

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 1.00062*

Threat Hunting

FortiAnalyzer *v6.4+*
FortiSIEM *v6.4+*

Content Update

FortiSIEM *DB 304+*

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

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

Additional Resources

Wordfence PSA https://www.wordfence.com/blog/2022/09/psa-zero-day-vulnerability-in-wpgateway-actively-exploited-in-the-wild/

The Hacker News https://thehackernews.com/2022/09/over-280000-wordpress-sites-attacked.html

Bleeping Computer https://www.bleepingcomputer.com/news/security/zero-day-in-wpgateway-wordpress-plugin-actively-exploited-in-attacks/

Learn more about FortiGuard Outbreak Alerts

FORTINET