FORTINET

OUTBREAK ALERTS

Generic Web Application Firewall (WAF) Security Bypass

Abusing JSON-Based SQL to Bypass WAF

https://claroty.com/team82/research/js-on-security-off-abusing-json-based-sql-to-bypass-waf

Recently, security researchers at Claroty posted a blog describing a method for bypassing some vendors WAF solutions. The attack technique involves appending JSON syntax to SQL injection payloads.

Background

The method described bypasses malicious requests that used JSON (JavaScript Object Notation) syntax appended to SQL injection payloads. Attackers could then use these techniques to get access to a backend database and use additional vulnerabilities to exfiltrate data via either direct access to the server or over the cloud.

Announced

December 8th, 2022: Claroty Team82 posted a research at:
https://claroty.com/team82/research/js-on-security-off-abusing-json-based-sql-to-bypass-waf

Latest Developments

Fortinet customers using the FortiWeb (Web Application Firewall) remain protected against these types of evasion techniques. FortiWeb ML for anomaly Detection protects against zero-day and such unknown attacks without requiring any special configuration.
https://www.fortinet.com/products/web-application-firewall/fortiweb

PROTECT

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

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

Anomaly Detection

Machine Learning feature protects against attack techniques related to WAF security bypass

FortiWeb

v7.0+

- Installation
- C2
- Action

DETECT

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

Threat Hunting

Machine Learning for Anomaly Detection against attack techniques related to WAF security bypass

FortiWeb

v7.0+

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:

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.

FortiPenTest

Additional Resources

Claroty	https://claroty.com/team82/research/js-on-security-off-abusing-json-based-sql-to-bypass-waf
FortiWeb	https://www.fortiweb-cloud.com/
Security Affairs	https://securityaffairs.co/wordpress/139445/hacking/web-application-firewalls-waf-bypass.html
Techtarget	https://www.techtarget.com/searchsecurity/news/252528217/Claroty-unveils-web-application-firewall-bypassing-technique

Learn more about FortiGuard Outbreak Alerts