FORTINET

OUTBREAK ALERTS

Redigo Attack

New Go-based Redigo malware targets Redis server

https://security-tracker.debian.org/tracker/CVE-2022-0543
CVEs: CVE-2022-0543

Go based malware that targets Redis server's vulnerability CVE-2022-0543 allowing threat actors to drop the Redigo malware and gain server access.

Background

Redis (remote dictionary server) is an open-source in-memory database and cache based on a Unix-like operating system. The server has a built-in Lua scripting engine that allows users to upload and execute Lua scripts directly on the server which helps users to efficiently perform the process read and writing data from scripts.

Previously, the same vulnerability CVE-2022-0543 was seen in a different malware attack called "Muhstik"
https://blogs.juniper.net/en-us/security/muhstik-gang-targets-redis-servers

Announced

February 18, 2022: Ubuntu published security advisory CVE-2022-0543 at
https://ubuntu.com/security/CVE-2022-0543

Latest Developments

December 01, 2022: Aqua Nautilus Discovers Redigo - A New Redis Backdoor Malware
https://blog.aquasec.com/redigo-redis-backdoor-malware

PROTECT

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

Reconnaissance

Weaponization

Delivery

AV

Detects malware payloads related to Redigo attack

FortiGate	FortiWeb	FortiClient	FortiSASE	FortiMail	FortiCASB	FortiCWP
DB 90.08462	DB 90.08462	DB 90.08462	DB 90.08462	DB 90.08462	DB 90.08462	DB 90.08462

FortiADC	FortiProxy
DB 90.08462	DB 90.08462

Vulnerability

Detects presence of Redis vulnerability on Linux machines

FortiClient
DB 2.088

AV (Pre-filter)

Detects malware payloads related to Redigo attack

FortiEDR	FortiSandbox
DB 90.08462	DB 90.08462

Behavior Detection

Behaviour Analysis engine rates Redigo malware as low risk, due to limited visibility of the nature of malware

FortiSandbox
v4.0+

Exploitation

IPS

Detects and block attack attempts related to Redis server vulnerability (CVE-2022-0543)

FortiGate	FortiSASE	FortiNDR	FortiADC	FortiProxy
DB 20.312	DB 20.312	DB 20.312	DB 20.312	DB 20.312

Application Firewall

Detects and block endpoint attack attempts related to Redis server vulnerability (CVE-2022-0543)

FortiClient
DB 21.341

Installation

Post-execution

Detects and blocks post exploitation activities related to Redigo Attack

FortiEDR
v4.0+

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

Detects and blocks post exploitation activities related to Redigo Attack

FortiEDR	FortiAnalyzer	FortiSIEM
v4.0+	v6.4+	v6.6.0+

Outbreak Detection

FortiAnalyzer
DB 1.00078

Content Update

FortiSIEM
DB 402

RESPOND

Develop containment techniques to mitigate impacts of security events:

Automated Response

Services that can automatically respond to this outbreak.

FortiClient Forensics	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:

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	FortiRecon: EASM	FortiDAST

Additional Resources

Debian Bug	https://bugs.debian.org/cgi-bin/bugreport.cgi?bug=1005787
Ubuntu Advisory	https://ubuntu.com/security/CVE-2022-0543
Security Week	https://www.securityweek.com/redigo-new-backdoor-targeting-redis-servers
The Hacker News	https://thehackernews.com/2022/12/hackers-exploiting-redis-vulnerability.html

Learn more about FortiGuard Outbreak Alerts