Lazarus RAT Attack

APT group exploiting Log4j2 vulnerability to deploy Remote Access Trojans (RAT) https://blog.talosintelligence.com/lazarus_new_rats_dlang_and_telegram/

CVEs: CVE-2021-44228 A new campaign conducted by the Lazarus Group is seen employing new DLang-based Remote Access Trojans (RATs) malware in the wild. The

APT groups has been seen to target manufacturing, agricultural and physical security companies by exploiting the Log4j vulnerability and using it for initial access leading to a C2 (command and control) channel with the attacker. **Background** Lazarus is an advanced persistent threat (APT) actor sponsored by the North Korean government. In this particular

Announced

Latest Developments

vulnerability discovered in 2021. Log4Shell is an unauthenticated remote code execution (RCE) flaw that allows taking complete control over systems using vulnerable versions of Log4j library. The flaw was discovered as an actively exploited zero-day on

campaign, Lazarus's initial access begins with successful exploitation of CVE-2021-44228, the infamous Log4j

December 10, 2021, and its widespread impact, ease of exploitation, and massive security implications acted as an open invitation to threat actors. To learn more please read the outbreak report: https://www.fortiguard.com/outbreak-alert/log4j2-vulnerability

December 11, 2023: Cisco Talos posted a blog and shared latest findings on; https://blog.talosintelligence.com/lazarus_new_rats_dlang_and_telegram

Fortinet customers remain protected by the IPS signature "Apache.Log4j.Error.Log.Remote.Code.Execution" and the Antivirus detections for the related Remote Access Trojans (RATs).

> actors are still actively targeting the log4j vulnerability and using it as an initial access due to its widespread usage. According to a report by Veracode, over 30% of Log4J apps still use a vulnerable version of the library after 2

> years of the patches being released and a log4j dashboard by Sonatype shows, 25% of the library's downloads in

of upto 65,000+ unique IPS devices. However, this particular campaign is just one of the instance where threat

December, 2023: According to the FortiGuard telemetry, there is a significant increased activity in the IPS detection

https://www.sonatype.com/resources/log4j-vulnerability-resource-center

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



Reconnaissance

Decoy VM

FortiDeceptor DB 20221105

AV

Detects presence of Log4j2 vulnerability

FortiSandbox

DB 91.09630

Blocks exploitation of the Log4j2 vulnerability

FortiSASE

DB 22.404

FortiWeb

DB 91.09630

FortiProxy

FortiClient

DB 91.09630

FortiSASE

DB 91.09630

FortiMail

DB 91.09630

FortiProxy

DB 22.404

FortiCASB

DB 91.09630

FortiCWP

DB 91.09630

v5.0+ Detects and blocks Remote Access Trojan (RATs) related to the Lazarus RAT Attack

FortiEDR

DB 91.09630

FortiClient

FortiNDR

DB 22.404

FortiADC

DB 22.404

FortiNDR

DB 91.09630

FortiGate

Blocks exploitation of the Log4j2 vulnerability



v5.0+

FortiEDR

DETECT

Outbreak Detection

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

FortiSIEM

DB 602

Threat Hunting

FortiClient

DB 1.00017

FortiEDR FortiAnalyzer v6.4+ v5.0+ Playbook

FortiAnalyzer

DB 2.00031

RESPOND

FortiSOAR

v7.4.+

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

Assisted Response Services

RECOVER

End-User Training Raise security awareness to your employees that are continuously being targetted by phishing, drive-by download and other forms of cyberattacks.

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



Security **FortiDAST** Rating

Vulnerability Management

FortiDevSec FortiEDR

Additional Resources

CISA Guidance https://www.cisa.gov/news-events/news/apache-log4j-vulnerability-guidance

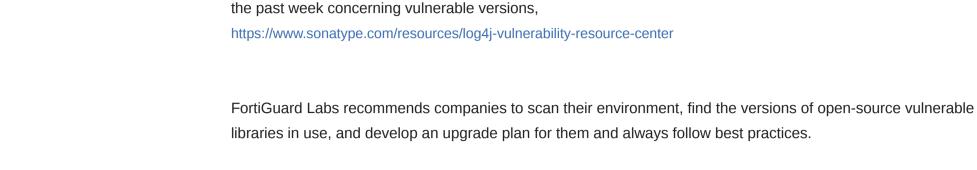
Reduce the attack surface on software vulnerabilities via systematic and automated patching.

The Hacker News https://thehackernews.com/2023/12/lazarus-group-using-log4j-exploits-to.html

Security Week https://www.securityweek.com/north-korean-hackers-developing-malware-in-dlang-programming-language/

Learn more about FortiGuard Outbreak Alerts





PROTECT

Detects activities related to the Log4j2 vulnerability

Weaponization **Delivery**

Detects and blocks Remote Access Trojan (RATs) related to the Lazarus RAT Attack

FortiADC

FortiGate DB 91.09630

> DB 91.09630 DB 91.09630 **Vulnerability**

AV (Pre-filter)

IPS

Exploitation

DB 22.404

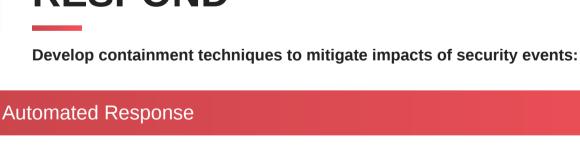
Web App Security

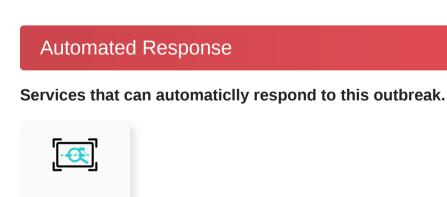
FortiWeb FortiADC DB 1.00030 DB 0.00308

C2 Action











FortiXDR



Incident Response



cyberattacks.

NSE Training

NOC/SOC Training

Response

Readiness

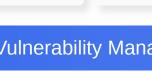


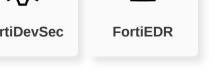
Awareness & Training





Identify processes and assets that need protection:







Dark Reading



