

This repository has been archived by the owner on Jun 16, 2022. It is now read-only.

Table of repository files and commits, including .github, detection_mitigation, hunting, iocs, scanning, software, tools, .gitignore, LICENSE, README.md, and log4shell_en.png.

README License

Log4shell vulnerabilities (CVE-2021-44228, CVE-2021-45046, CVE-2021-4104, CVE-2021-45105)

This repo contains operational information regarding the Log4shell vulnerability in the Log4j logging library. Especially CVE-2021-44228 / CVE-2021-45046 and also covers CVE-2021-4104 / CVE-2021-45105. For additional information see:

- NCSC-NL advisory
MITRE
EU CSIRT network members advisories, maintained by ENISA
Log4shell vulnerability overview

For affected organisations and CISOs searching for concise mitigation guidance, the Log4Shell for OES - Full presentation slides for CISOs and techies describes the vulnerability and explains all steps necessary to successfully mitigate the vulnerability (patching is not enough).

Repository contents

Table with 2 columns: Directory and Purpose. Rows include hunting, iocs, detection & mitigation, scanning, software, and tools.

Please note that these directories are not complete, and are currently being expanded.

NCSC-NL has published a HIGH/HIGH advisory for the Log4j vulnerability. Normally we would update the HIGH/HIGH advisory for vulnerable software packages, however due to the extensive amounts of expected updates we have created a list of known vulnerable software in the software directory.

Contributions welcome

If you have any additional information to share relevant to the Log4j vulnerability, please feel free to open a Pull request. New to this? Read how to contribute in GitHub's documentation.

Hall of fame

We would like to thank every single one of you that contributed to our GitHub page. NCSC-NL believes the GitHub page is a succes and you made that possible. Below we present a very incomplete list of contributants we consider the repository's hall of fame:

- ANSSI
BSI/CERT-Bund
CERT-EU
Cybersecurity & Infrastructure Security Agency CISA
DCSC
SURFcert
SK-CERT
Z-CERT
@DFFSpace
@tintinhamans
@milankowww
@MrSeccubus
@Goldshop
@RemkoSikkema
@MetzieNL
@RobinFlikkema
@lucasjellema
@iglocska

About

Operational information regarding the log4shell vulnerabilities in the Log4j logging library.

- log4j vulnerability cve-2021-44228
log4shell cve-2021-45046
cve-2021-4104 cve-2021-45105

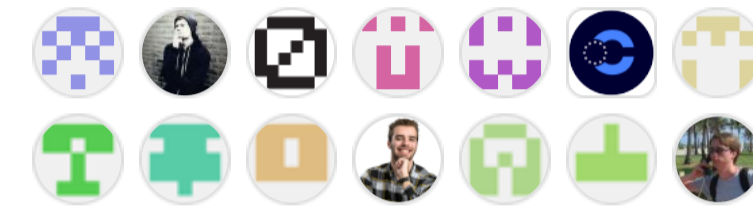
- Readme
Activity
Custom properties
1.9k stars
69 watching
611 forks

Releases 163

log4shell_info_20220615 Latest on Jun 16, 2022

+ 162 releases

Contributors 275



+ 261 contributors

Languages

Python 100.0%