Basque CyberSecurity Centre

Kalteberatasunak Apache commons_text-en eta commons_configuration-en (CVE-2022-42889, CVE-2022-0030)

BCSC-ABISUAK

TLP: CLEAR

www.zibersegurtasun.eus

EUSKO JAURLARITZA GOBIERNO VASCO

GRUPO spri TALDEA

EDUKIAREN TAULA

BCSCri buruz 3
1. Segurtasun-abisua 4
2. Eragindako baliabideak 5
3. Analisi teknikoa 6
4. Arintzea / Konponbidea 8
5. Erreferentzia gehigarriak 9

Erantzukizunetik salbuesteko klausula

Dokumentu hau ematen da BCSCk erakundeen eta herritar interesdunen segurtasunaren alde beharrezkotzat jotzen dituen alertak zabaltzeko. BCSC ezin da inola ere jo zuzenean edo zeharka, ustekabean edo ohiz kanpo, jakinarazitako informazioa erabiltzeak eragin ditzakeen kalteen erantzuletzat, ez eta BCSCren webgunetik nahiz kanpoko informaziotik (kanpoko web-orrietarako, sare sozialetarako, software-produktuetarako edo BCSCren alertaren edo webgunearen bidez ager daitekeen beste edozein informaziotarako esteken bidez) aipatzen diren teknologien erantzuletzat ere. Nolanahi ere, alertaren edukiak eta mezu elektronikoen bidez eman daitezkeen erantzunak hemen jasotako terminoen araberako iritziak eta gomendioak dira, eta ezingo da ondorio juridiko loteslerik sortu jakinarazitako informaziotik.

Saltzeko debekuaren klausula

BCSCri buruz

Zibersegurtasunaren Euskal Zentroa (Basque Cybersecurity Centre, BCSC) Eusko Jaurlaritzak zibersegurtasunaren heldutasun-maila handitzeko izendatutako erakundea da.

Zeharkako ekimena da, Eusko Jaurlaritzako Ekonomiaren Garapen, Jasangarritasun eta Ingurumen Sailaren mendekoa den Enpresen Garapenerako Euskal Agentziaren (SPRI) barruan dagoena. Era berean, Eusko Jaurlaritzako beste hiru sail ere sartzen dira ekimenean –Segurtasuna, Gobernantza Publikoa eta Autogobernua eta Hezkuntza Saila–, eta Zientzia, Teknologia eta Berrikuntzaren Euskal Sareko lau eragile: Tecnalia, Vicomtech, Ikerlan eta BCAM.

BCSC erreferentzia-erakundea da Euskadiko herritarren, enpresen eta erakunde publikoen zibersegurtasuna eta konfiantza digitala garatzeko, bereziki eskualdeko ekonomiaren sektore estrategikoentzat.

BCSCren egitekoa da, beraz, euskal gizartean zibersegurtasuna sustatzea eta garatzea, Euskadiko enpresa-jarduera dinamizatzea eta erreferentea izango den sektore profesional bat sortzea ahalbidetzea. Testuinguru horretan, eragile osagarrien arteko lankidetza-proiektuak gauzatzea bultzatzen da, berrikuntza teknologikoaren, ikerketaren eta fabrikazio aurreratuko industriarako eta beste sektore batzuetarako transferentzia teknologikoaren eremuetan.

Era berean, hainbat zerbitzu eskaintzen ditu Gorabeherei erantzuteko lantalde gisa (aurrerantzean CERT: “Computer Emergency Response Team” ingelesezko siglak), eta Euskal Autonomia Erkidegoaren esparruan lan egiten du mehatxu berriak detektatzeko eta garaiz ohartarazteko gaitasuna handitzen, informazioaren segurtasun-gorabeheren erantzuna eta analisia egiten, eta euskal gizartearen beharrei erantzuteko prebentzio-neurriak diseinatzen. Helburu horiek lortzeko, zibersegurtasun-gorabeherak kudeatzera bideratutako hainbat ekimenen parte da:

FIRST Improving Security Together
TF-CSIRT Trusted Introducer
CSIRT.es

1. Segurtasun-abisua

Urriaren 28an,Apache Commons_text-i eragiten dioten bi kalteberatasun kritiko jakinarazi ziren, CVE-2022-42889 identifikatzailearekin, eta Apache commons_configuration-i, CVE-2022-33980 identifikatzailearekin.

Hainbat fabrikatzailek jakinarazi dute segurtasun-hutsegite horiek Fortinet, SonicWall edo netAPP bezalako produktuetan duten inpaktua.

Ez dakigu kalteberatasunak aktiboki ustiatzen ari diren edo garatutako exploit bat dagoen, gaur egun.

2. Eragindako baliabideak

- Apache Commons Text-en 1.5 bertsioa, 1.9 arte
- Apache commons_configuration-en 2.4 bertsioa, 2.7 arte

3. Analisi teknikoa

CVE-2022-42889 identifikatzailea duen kalteberatasunak Apache Commons Text liburutegiari eragiten dio, aldagaien interpolazioa egiten duen liburutegia, propietateak modu dinamikoan ebaluatu eta zabaltzeko aukera ematen duena. Interpolaziorako formatu estandarra *"${aurrizkia:izena}"* da. Bertan, "aurrizkia" erabiltzen da apache.commons.text.lookup.StringLookup-en honen instantzia bat kokatzeko, interpolazioa egiten duena. **1.5 bertsioarekin hasi eta 1.9 arte jarraituz, aurrez zehaztutako bilaketa-instantzien multzoak barne hartzen zituen interpoladoreak, kode arbitrarioaren exekuzioa edo urruneko zerbitzariekiko kontaktua sor zezaketenak**. Hauek dira bilaketak: - "script": espresioak exekutatzen ditu JVM scripten (javax.script) exekuzio-motorra erabiliz - “dns”: dns erregistroak ebazten ditu - "url”: URLtik baloreak kargatzen ditu, baita urruneko zerbitzarietatik ere **Eragindako bertsioetan aurrez zehaztutako interpolazio-balioak erabiltzen dituzten aplikazioak kodearen urruneko exekuzioarekiko edo urruneko zerbitzariekiko nahigabeko kontaktuarekiko kalteberak izan daitezke konfiantzazkoak ez diren konfigurazio-balioak erabiltzen badira**.

Kalteberatasuna ebaluatzeko metrika hau da:

CVSS Base: 9.8. Kritikoa

CWE-94: Improper Control of Generation of Code ('Code Injection')

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

- **Eraso-bektorea**: **Sarea**
- **Erasoaren konplexutasuna**: **Txikia**
- **Eskatutako pribilegioak: Bat ere ez**
- **Erabiltzailearekiko interakzioa**: **Bat ere ez**
- **Irismena**: Aldaketarik gabe
- **Konfidentzialtasuna: Handia**
- **Osotasuna: Handia**
- **Erabilgarritasuna: Handia**

CVE-2022-33980 -ri dagokionez , aldagaien interpolazioa egiten duen Apache Commons-en konfigurazioari eragiten dio , eta horrek propietateak dinamikoki ebaluatu eta zabaltzeko aukera ematen du Interpolaziorako formatu estandarra "${prefix:name}" da, eta bertan "prefix" erabiltzen da interpolazioa egiten duen apache.commons.configuration2.interpol.Lookup.-en instantzia bat kokatzeko. **2.4 bertsioarekin hasi eta 2.7 bertsiora arte jarraituta, aurrez zehaztutako bilaketa-instantzien multzoak barne hartzen zituen interpoladoreak, kode arbitrarioaren exekuzioa edo urruneko zerbitzariekiko kontaktua sor zezaketenak**. Hauek dira bilaketak: - "script": espresioak exekutatzen ditu JVM scripten (javax.script) exekuzio-motorra erabiliz - “dns”: dns erregistroak ebazten ditu - "url”: URLtik baloreak kargatzen ditu, baita urruneko zerbitzarietatik ere

Eragindako bertsioetan aurrez zehaztutako interpolazio-balioak erabiltzen dituzten aplikazioak kodearen urruneko exekuzioarekiko edo urruneko zerbitzariekiko nahigabeko kontaktuarekiko kalteberak izan daitezke konfiantzazkoak ez diren konfigurazio-balioak erabiltzen badira.

Kalteberatasuna ebaluatzeko metrika hau da:

CVSS Base: 9.8. Kritikoa

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

- **Eraso-bektorea**: **Sarea**
- **Erasoaren konplexutasuna**: **Txikia**
- **Eskatutako pribilegioak: Bat ere ez**
- **Erabiltzailearekiko interakzioa**: **Bat ere ez**
- **Irismena**: Aldaketarik gabe
- **Konfidentzialtasuna: Handia**
- **Osotasuna: Handia**
- **Erabilgarritasuna: Handia**

4. Arintzea / Konponbidea

Kalteberatasun hori arintzeko, BCSCk gomendatzen du sistema eta aplikazioak erabilgarri dagoen azken bertsiora eguneratuta edukitzea beti, dagozkion eguneratzeak argitaratu bezain laster.

- ✓ CVE-2022-42889 hutsegitea konpontzeko, erabiltzaileei ApApache Commons Text 1.10.0-ra eguneratzea gomendatzen zaie, interpoladore problematikoak modu lehenetsian desaktibatzen baititu.
- ✓ CVE-2022-33980 ari dagokionez, erabiltzaileei Apache Commons Configuration 2.8.0-ra eguneratzea gomendatzen zaie, interpoladore problematikoak modu lehenetsian desaktibatzen baititu.

5. Erreferentzia gehigarriak

- CVE-2022-42889
- CVE-2022-33980
- Apache Commons Text
- Apache commons_configuration
- CWE-94: Improper Control of Generation of Code ('Code Injection')
- Fortinet
- SonicWall
- netAPP


Basque
CyberSecurity
Centre


EUSKO JAURLARITZA
GOBIERNO VASCO


GRUPO
spri
TALDEA