Kalteberatasunak Atlassian produktuetan

CYBERZAINTZA-ABISUAK

TLP: CLEAR

www.zibersegurtasun.eus

EDUKI-TAULA

Erantzukizunetik salbuesteko klausula

Dokumentu hau BCSCk interesdun erakundeen eta herritarren segurtasunaren alde beharrezkotzat jotzen dituen alertak gizarteratzeko helburuz sortu da. BCSC ezin da jo, inola ere, BCSCren webgunean emandako informazioaren edo erreferentzia egiten zaien teknologien erabilerak eragin ditzaketen kalteen erantzuletzat, ezta kanpoko web-orrialdeetarako esteka bidez sartutako bestelako informazioaren, software produktuen edo BCSCren webgunean edo alertan ager daitezkeen beste edozein informazioaren erantzuletzat ere. Edonola ere, alertaren edukiak eta mezu elektronikoen bidez eman litezkeen erantzunak iritzi eta gomendioak dira, hemen bildutako terminoekin bat etorrita, eta emandako informazioaren ondorioz ezingo da eragin juridiko loteslerik sortu.

Salmenta debekatzeko klausula

1. Laburpen exekutiboa

Atlassianek hilabeteko segurtasunaren eguneraketa argitaratu du eta hainbat kalteberatasun jorratzen dira bertan: bat larritasun kritikokoa da eta besteak larritasun handikoak. **Bamboo Data Center and Server, Bitbucket Data Center and Server** eta **Confluence Data Center and Server** produktuei eragiten diete.

Jorratutako kalteberatasun berri esanguratsuenen identifikatzaileak hauek dira: CVE-2024-1597, CVE-2024-21634 eta CVE-2024-21677 Horietako guztiak ustiatzea larritasun handiko mehatxua da kaltetutako sistemen erabilgarritasunerako. Lehenengoaren kasuan, konfidentzialtasuna eta osotasuna ere arriskuan daude.

CVE-2024-1597 kalteberatasunari dagokionez, nabarmentzekoa da Atlassianen ez den Bambooren dependentzia bateko **larritasun kritikoko akatsa** dela. Hala ere, Atlassianen mendeko aplikazioak ebaluatutako arrisku txikiagoa du, horregatik zabaldu da kalteberatasuna Atlassianen hileko Segurtasuneko Aldizkarian eta ez da Segurtasun Abisu kritikorik igorri.

Fabrikatzaileak dagoeneko argitaratu ditu dagozkion eguneratzeak eta arintze-neurriak, eta, horrela, akats nabarmenak zuzendu ditu. Beraz, kalteberatasun horiek eta beste batzuk prebenitzeko, sistema eta aplikazioak eskuragarri dagoen azken bertsioaren arabera eguneratuta izatea gomendatzen da, dagozkien adabakiak argitaratu bezain laster.

2. Kaltetutako baliabideak

- Confluence Data Server.
- Bamboo Data Center eta Server.
- Bitbucket Data Center eta Server.

3. Azterketa teknikoa

Abisu honetan landutako kalteberatasun garrantzitsuenen xehetasunak hauek dira:

CVE-2024-1597: Bamboo Data Center eta Serverren SQL injektatzen duen kalteberatasun kritikoa da eta egiaztatu gabeko erasotzaile batek bere inguruneko ustia daitezkeen aktiboak erakutsi ditzake, konfidentzialtasunean eragin handia dutenak, integritatean eragin handia dutenak, erabilgarritasunean eragin handia dutenak eta erabiltzailearen interakziorik behar ez dutenak.

Kalteberatasunaren azterketaren neurketak honako hauek ditu:

Oinarrizko CVSSa: **10**

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

- **Eraso-bektorea: Sarea**
- **Erasoaren konplexutasuna**: **Baxua**
- **Beharrezko pribilegioak: Bat ere ez**
- **Interakzioa erabiltzailearekin: Bat ere ez**
- **Irismena**: **Aldaketekin**
- **Konfidentzialtasuna Altua**
- **Integritatea: Altua**
- **Eskuragarritasuna: Altua**

CVE-2024-21677: Larritasun handiko Path Transversaleko kalteberatasuna da eta Confluence Data Centerri eragiten dio. Horren bidez, egiaztatu gabeko erasotzaile batek konfidentzialtasunean inpaktu handia, osotasunean inpaktu handia, eskuragarritasunean inpaktu handia eta erabiltzailearen interakzioa behar duen definitu ezin daitekeen kalteberatasuna ustia dezake.

Kalteberatasunaren azterketaren neurketak honako hauek ditu:

Oinarrizko CVSSa: **8.3**

CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:H

- **Eraso-bektorea: Sarea**
- **Erasoaren konplexutasuna**: **Altua**
- **Beharrezko pribilegioak: Bat ere ez**
- **Interakzioa erabiltzailearekin:** Beharrezkoa
- **Irismena**: **Aldaketekin**
- **Konfidentzialtasuna Altua**
- **Integritatea: Altua**
- **Eskuragarritasuna: Altua**

CVE-2024-21634: Bamboo Data Center eta Bitbucket Data Center eta Serverri eragiten dion kalteberatasun kritikoa da eta zerbitzua ukatzen du (DoS). Horren bidez, egiaztatu

gabeko erasotzaile batek bere inguruneko ustia daitezkeen aktiboak erakutsi ditzake, konfidentzialtasunean eraginik ez dutenak, integritatean eraginik ez dutenak, erabilgarritasunean eragin handia dutenak eta erabiltzailearen interakziorik behar ez dutenak.

Kalteberatasunaren azterketaren neurketak honako hauek ditu:

Oinarrizko CVSSa: **7.5**

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

- **Eraso-bektorea: Sarea**
- **Erasoaren konplexutasuna**: **Baxua**
- **Beharrezko pribilegioak: Bat ere ez**
- **Interakzioa erabiltzailearekin: Bat ere ez**
- **Irismena**: Aldaketarik gabe
- **Konfidentzialtasuna** Bat ere ez
- **Integritatea:** Bat ere ez
- **Eskuragarritasuna: Altua**

4. Arintzea / Konponbidea

Ohikoa den bezala, kalteberatasun horiek eta beste batzuk prebenitzeko, sistemak eta aplikazioak beti eskuragarri dagoen azken bertsiora eguneratuta izatea gomendatzen da, dagozkien eguneratzeak argitaratu bezain laster.

Ahultasun guztiak zuzentzeko, Atlassianek bere instantziei adabakiak aplikatzea gomendatzen du, azken bertsiora eguneratzeko. Ezin bada egin, jarraian adierazten diren gutxieneko zuzenketa-bertsioaren eguneratzeak aplikatu behar dira:

- **Bamboo Data Center eta Server**: Atlassianek azken bertsioa eguneratzea gomendatzen du, eta, bestela, bertsio finko espezifikoetako baten instantzia eguneratzea.

- **Confluence Data Center eta Server**: Atlassianek azken bertsioa eguneratzea gomendatzen du. Bestela, instantzia bertsio finko bateragarri espezifikoetako batera eguneratzea.

- **Bitbucket Data Center eta Server**: Atlassianek azken bertsioa eguneratzea gomendatzen du, eta, bestela, bertsio finko espezifikoetako baten instantzia eguneratzea.

5. Erreferentzia gehigarriak

- Hileko segurtasun-eguneraketa.
- CVE-2024-1597.
- CVE-2024-21634.
- CVE-2024-21677.


cyber
zaintza
BASQUE CYBERSECURITY AGENCY