TRABAJO 1 CIBERSEGURIDAD

LUIS ALBERTO ÁLVAREZ ZAVALETA

Índice

Motivación

La realización de este trabajo está enfocada en abordar 5 "security issues" de los últimos años y el impacto que estos han tenido para salvaguardar la integridad, confidencialidad y disponibilidad de los sistemas afectados

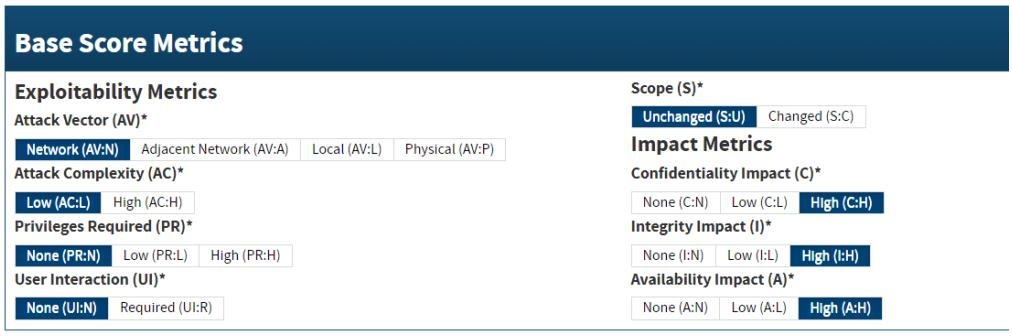
En cada uno de estos trabajos se describirá el caso, dando detalles del tipo de vulnerabilidad que se ha dado y describiendo un poco sobre el impacto que ha tenido, el vector de ataque que se ha utilizado y el tipo de repercusiones que ha tenido. Además, se realizará una lista con las medidas de mitigación que se han tomado antes de que esta vulnerabilidad se hubiese parcheado.

Security Issues

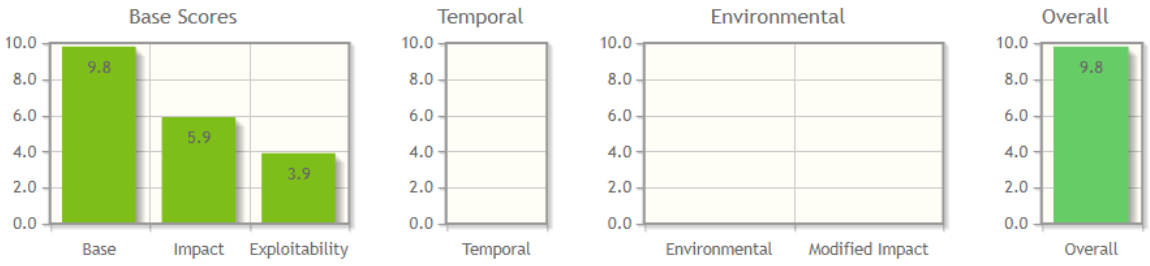
CVE-2022-22965

Una aplicación Spring MVC o Spring WebFlux que es ejecutada en JDK 9+ puede ser vulnerable a la ejecución de código remota (RCE). La explotación específica requiere que la aplicación sea ejecutada en Tomcat como un despliegue WAR. Si la aplicación es desplegada como un jar ejecutable de Spring Boot, es decir, por defecto, no es vulnerable a la explotación. Sin embargo, la naturaleza de la vulnerabilidad es más general, y puede haber otras formas de explotarla

Spring es uno de los frameworks de código abierto más conocidos esto implica que un gran número de aplicaciones empresariales podrían verse afectadas. La popularidad de Spring significa y el hecho de que la vulnerabilidad esté relacionada con la ejecución de código remoto (RCE) plantea riesgos significativos para la seguridad de las empresas.



La posibilidad de ejecutar código de manera remota sin tener la necesidad de privilegios, en una aplicación puede conducir a consecuencias graves, como la pérdida de datos confidenciales, interrupciones en los servicios y, en última instancia, daños a la reputación de la empresa.



Entre posibles medidas para mitigar la vulnerabilidad se propusieron los siguientes

- Bloquear las conexiones entrantes y salientes entre el sistema e Internet hasta que se despliegue el parche de corrección
- Actualizar Tomcat, ya que aplicaron un parche para evitar esta vulnerabilidad desde tomcat
- Hacer un Dowgrade a Java 8
- Deshabilitar determinados campos en las peticiones

CVE-2023-4418

Este cve se produjo por un fallo criptográfico que causaba que la librería OpenSSL entre en un bucle infinito cuanto intentaba parsear un certificado invalido, causando que el atacante pudiera realizar una denegación de servicio contra el dispositivo LMS5xx que tuviese esta vulnerabilidad.

El LMS5xx es un sensor LiDAR 2D potente diseñado para la detección precisa de objetos a largas distancias. Este tipo de sensores se utilizan en distintos tipos de entornos de trabajo, desde sistemas de seguridad y vigilancia, hasta vehículos autónomos o cartografía o robótica.

Base Score Metrics

Exploitability Metrics

Attack Vector (AV)*
Network (AV:N) | Adjacent Network (AV:A) | Local (AV:L) | Physical (AV:P)

Attack Complexity (AC)*
Low (AC:L) | High (AC:H)

Privileges Required (PR)*
None (PR:N) | Low (PR:L) | High (PR:H)

User Interaction (UI)*
None (UI:N) | Required (UI:R)

Scope (S)*
Unchanged (S:U) | Changed (S:C)

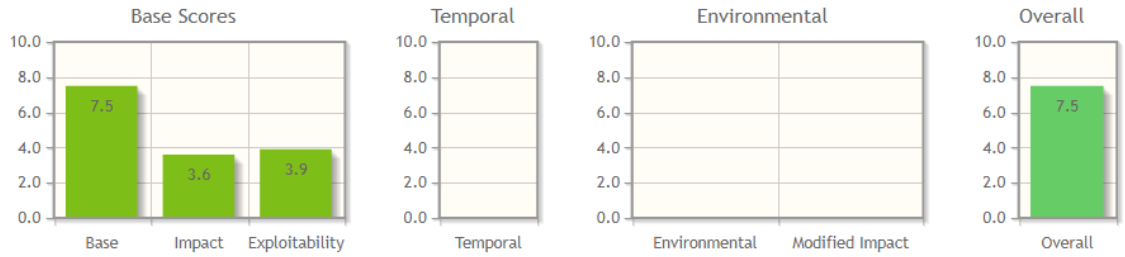
Impact Metrics

Confidentiality Impact (C)*
None (C:N) | Low (C:L) | High (C:H)

Integrity Impact (I)*
None (I:N) | Low (I:L) | High (I:H)

Availability Impact (A)*
None (A:N) | Low (A:L) | High (A:H)

El fallo de uno de estos servicios puede ser importante en algunos de estos dispositivos, y dado que se puede realizar el ataque desde la red, este tipo de ataque puede ser peligroso según la tarea que este realice.



Entre posibles medidas para mitigar la vulnerabilidad se encontraron los siguientes

- Desconectar temporalmente el dispositivo a internet
- Limitar el acceso ciertas direcciones red
- Seguir el manual General Security Practices and Operating Guidelines LMS5xx[1]

CVE-2023-22506

Se introdujo una vulnerabilidad crítica de Inyección y Ejecución Remota de Código (RCE), en la versión 8.0.0 de Bamboo Data Center. Atlassian recomendó actualizar a una de las versiones corregidas: 9.2.3 o 9.3.1. Puede encontrar información detallada en las notas.

Bamboo es una herramienta de integración y despliegue continuos (CI/CD) desarrollada por Atlassian. Su propósito principal es automatizar el proceso de compilación, prueba y despliegue de aplicaciones, lo que contribuye a un desarrollo de software más eficiente y confiable, Bamboo contiene una integración con herramientas como Jira y Bitbucket, por lo que es

[1] : https://cdn.sick.com/media/docs/7/17/717/technical_information_lms5xx_hardening_guide_en_im0106717.pdf

necesario considerar el impacto en la seguridad de todo el entorno de desarrollo que se haya visto comprometido.

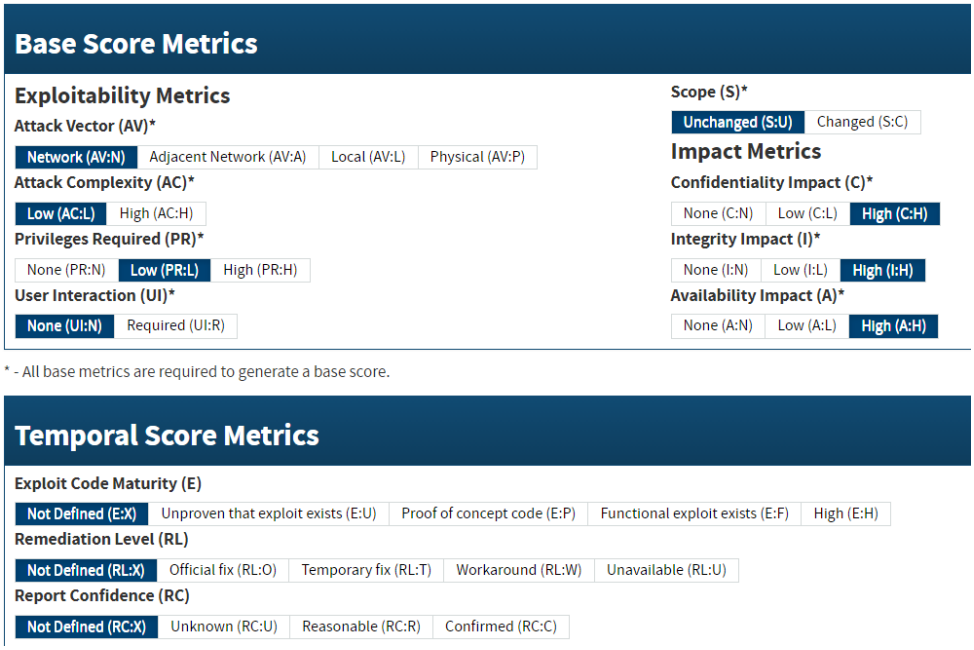
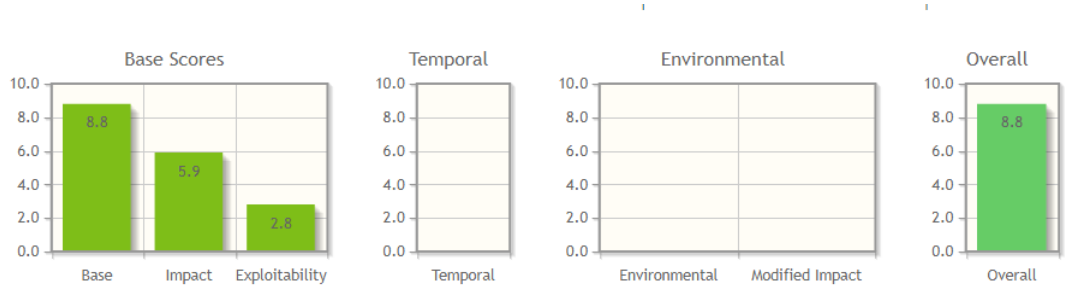


Ilustración 1.Base Score CVE-2023-22506 National Vulnerability Database

Esta vulnerabilidad, evaluada con un puntaje CVSS de 8.8 según la NVD, permite a atacantes autenticados manipular llamadas al sistema, ejecutando código arbitrario con impactos significativos en la confidencialidad, integridad y disponibilidad, sin requerir interacción del usuario. Además de que no se pudieron ofrecer mitigaciones por parte de los usuarios, fue necesario actualizar a la nueva versión de Bamboo con el parche de la vulnerablilidad



CVE-2022-21449

Una vulnerabilidad de tipo Broken Access Control que permite a un atacante no autenticado con acceso a la red, a través de múltiples protocolos comprometer Oracle Java SE, Oracle GraalVM Enterprise Edition.

Los ataques exitosos de esta vulnerabilidad pueden resultar en la creación no autorizada, eliminación o modificación de acceso a datos críticos de todos los datos accesibles en Oracle Java SE, Oracle GraalVM Enterprise Edition.

Base Score Metrics

Exploitability Metrics

Attack Vector (AV)*

Network (AV:N)	Adjacent Network (AV:A)	Local (AV:L)	Physical (AV:P)

Attack Complexity (AC)*

Low (AC:L)	High (AC:H)

Privileges Required (PR)*

None (PR:N)	Low (PR:L)	High (PR:H)

User Interaction (UI)*

None (UI:N)	Required (UI:R)

Scope (S)*

Unchanged (S:U)	Changed (S:C)

Impact Metrics

Confidentiality Impact (C)*

None (C:N)	Low (C:L)	High (C:H)

Integrity Impact (I)*

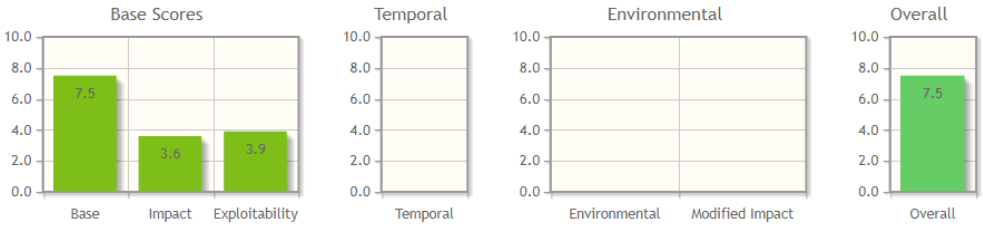
None (I:N)	Low (I:L)	High (I:H)

Availability Impact (A)*

None (A:N)	Low (A:L)	High (A:H)

Esta vulnerabilidad provenía de la implementación de Java de la verificación de firma ECDSA en la librería openjdk-17, en ella se encuentran dos valores, llamados r y s.

La implementación de Java de la verificación de firma ECDSA no verificaba si r o s eran mayores que cero, por lo que podía producir un valor de firma en el que ambos son 0 y Java lo aceptaría como una firma válida para cualquier mensaje y para cualquier llave pública.



CVE-2022-30190

Es una vulnerabilidad de Ejecución de código remoto Microsoft Office en la que el documento utiliza la función de descargar una plantilla remota de Word para recuperar un archivo HTML de un servidor web remoto, que a su vez utiliza el MSProto ms-msdt para descargarlo.

Base Score Metrics

Exploitability Metrics

Attack Vector (AV)*

Network (AV:N) | Adjacent Network (AV:A) | **Local (AV:L)** | Physical (AV:P)

Attack Complexity (AC)*

Low (AC:L) | High (AC:H)

Privileges Required (PR)*

None (PR:N) | Low (PR:L) | High (PR:H)

User Interaction (UI)*

None (UI:N) | **Required (UI:R)**

Scope (S)*

Unchanged (S:U) | Changed (S:C)

Impact Metrics

Confidentiality Impact (C)*

None (C:N) | Low (C:L) | **High (C:H)**

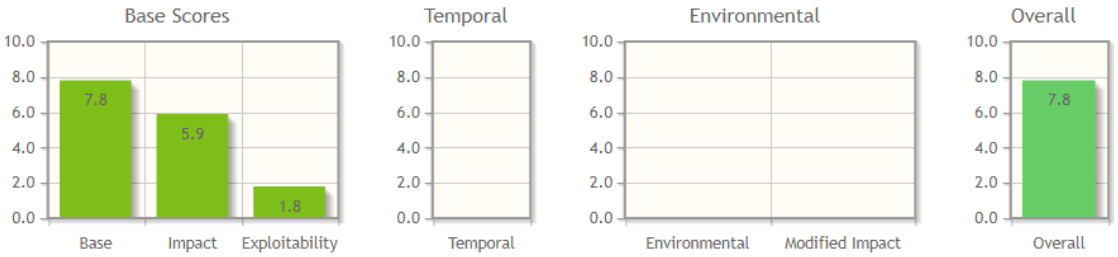
Integrity Impact (I)*

None (I:N) | Low (I:L) | **High (I:H)**

Availability Impact (A)*

None (A:N) | Low (A:L) | **High (A:H)**

MSDT podía permitir a personas no autorizadas acceder a componentes vitales de un sistema Windows. Podían manipular, recuperar o incluso destruir información crítica mediante la ejecución remota de código.



Dado que esta ejecución necesitaba la interacción del usuario a la hora de aplicar una plantilla, la vulnerabilidad era más difícil de ejecutarse. Entre algunos de las medidas que se propusieron para mitigar la vulnerabilidad se encuentran:

- Deshabilitar el protocolo URL de MSDT
- Tener actualizados antivirus y firewalls

Conclusiones

Este trabajo ha sido muy interesante a la hora de aprender más sobre posibles fallos de ciberseguridad que están sucediendo en la actualidad. Este tema es crucial, ya que la ciberseguridad desempeña un papel fundamental en nuestra sociedad cada vez más digitalizada.

Ha sido útil para comprender los riesgos y aprender sobre las prácticas que estas empresas adoptan para minimizar los fallos en ataques exitosos. Además de conocer como se han producido estos fallos para tenerlos en cuenta.

Bibliografía

https://nvd.nist.gov/vuln/detail/cve-2022-22965

https://nvd.nist.gov/vuln/detail/CVE-2023-4418

https://nvd.nist.gov/vuln/detail/CVE-2023-22506

https://nvd.nist.gov/vuln/detail/CVE-2022-21449

https://www.hackthebox.com/blog/cve-2022-30190-follina-explained

https://ciberseguridad.blog/analizando-y-explotando-follina-msdt-cve-2022-30190/

https://cdn.sick.com/media/docs/7/17/717/technical_information_lms5xx_hardening_guide_en_im0106717.pdf