Marín Parra José Guadalupe de Jesús

Conceptos básicos.

Contesta las siguientes preguntas.

1. ¿Quién administra la asignación de CVE?
   Respuesta.
   Las autoridades de numeración de CVE (CNA), asignan un número de identificación de CVE a la información además de incluirle una descripción y referencias.

2. ¿Qué proceso se debe realizar para reportar un CVE?
   Respuesta.
   Primero es la *Identifición* en donde se buscan vulnerabilidades por parte de investigadores o auditores; Después viene el *Reporte* en donde se envía la vulnerabilidad a CERT para informar al fabricante afectado y empezar con las acciones para la resolución de tal vulnerabilidad; A continuación es en *Análisis* en donde se confirma la vulnerabilidad por parte del CERT y se solicita información al informante de la vulnerabilidad; Después es el *Tratamiento* en donde se clasifica la vulnerabilidad usando métricas CVSS y se asigna un código CVE; Finalmente se hace la *Publicación* en donde se publica la vulnerabilidad a través de un canal oficial para informar a los clientes del fabricante acerca de los problemas detectados.

3. ¿Quién administra los CWE?
   Respuesta.
   Mitre Corporation es propietaria además de mantener y administrar el CWE.

4. ¿Qué diferencias hay entre la especificación actual de CVSS (3.0) y la anterior?
   Respuesta.

   - En la versión 3.0 se incluye una métrica denominada 'Alcance' para identificar vulnerabilidades más específicamente.
   - Se sustituye la métrica 'Vector de acceso' de la version 2.0 con la métrica 'Vector de ataque' la cual es más precisa en cuanto a los escenarios de una vulnerabilidad.
   - En la versión 3.0 se separó la métrica 'Complejidad de acceso' (de la versión 2.0) en 'Complejidad de ataque' la cual se refiere a cómo el atacante puede explotar la vulnerabilidad y en 'Interacción con el usuario' en donde se considera al usuario para medir la efectividad de un ataque.
   - En la versión 3.0 se reemplazó la métrica 'Autenticación' de la versión 2.0 por la métrica 'Privilegios requeridos' en donde se evalúan los privilegios necesarios para lograr un propósito ofensivo.
   - En la versión 2.0 el impacto a la confidencialidad, integridad y disponibilidad se categorizaba como nulo, parcial o completo mientras que en la versión 3.0 se categoriza como nulo, bajo y alto.

Marín Parra José Guadalupe de Jesús

Vulnerabilidades en sistemas.

Investiga tres CVE del año en curso de cada uno de los sistemas revisados en la tarea anterior. Explica **con tus propias palabras** cada CVE escogido, así como las medidas (si hay) que se hayan desarrollado para mitigar la vulnerabilidad (parches, hotfix, cambios de configuración, etc.)

Respuesta.

1. **Sharepoint**.
   - ID: CVE-2022-38009. Vulnerabilidad que consiste en ejecución remota de código en Sharepoint. No hay soluciones alternativas para esta vulnerabilidad.
   - ID: CVE-2022-27167. En los instaladores de Sharepoint para Windows había una vulnerabilidad la cual permitía que un usuario que iniciaba sesión podía realizar ataques que modificaban sus privilegios en la aplicación. La solución fue una actualización para cubrir la vulnerabilidad.
   - ID: CVE-2022-24472. Vulnerabilidad que consiste en la suplantación de identidad en Sharepoint Server. No hay soluciones alternativas para esta vulnerabilidad.
2. **Confluence**.
   - ID: CVE-2022-26138. En cofluence server se puede crear una cuenta de usuario con el username 'disabledsystemuser' y una contraseña cualquiera la cual está codificada, la vulnerabilidad consiste en que un atacante que sepa cuál es la contraseña puede iniciar sesión en cofluence y acceder a todos los datos que se encuentran en grupos de usuarios de cofluence. No hay soluciones alternativas para esta vulnerabilidad.
   - ID: CVE-2022-26137. Vulnerabilidad la cual permite que un atacante sin autentificación pueda evitar pasar por los filtros de los servlets causando que éste pueda realizar ataque tipo XSS. Se han publicado nuevas versiones para tratar la vulnerabilidad.
   - ID: CVE-2022-26134. En las versiones de cofluence existe una vulnerabilidad de inyección de OGNL la cual permitía a los atacantes ejecutar código en una instancia de cofluence server. La solución para tal vulnerabilidad fue una actualización.
3. **Jira**.
   - ID: CVE-2022-39960. Existía un complemento llamado 'Netic Group Export' en el cual Jira no realizaba comprobaciones de autorización lo que permitía a los usuarios no autenticados exportar todos los grupos de la instancia de Jira. La solución fue aplicar un parche para solucionar el bug.
   - ID: CVE-2022-36801. Vulnerabilidad que permitía a los atacantes inyectar código HTML o JavaScript a través de secuencias de comando cruzadas reflejadas (RXSS). La solución fue una actualización a la versión.
   - ID: CVE-2022-36799. Las versiones anteriores de Jira, permitían a los atacantes ejecutar código como administradores a través de plantillas de correo electrónico. La solución fue una actualización a la versión.
4. **Zendesk**.
   Para este sistema no hay CVE's del año en curso razón por la cual agregaré las más recientes.
   - ID: CVE-2018-20857. Vulnerabilidad en la cual un atacante podía realizar ataques a los comentarios de los nodos XML con un nodo del ID de un nombre y el correo de un usuario seguido del nombre del dominio del atacante. La solución fue una actualización a la versión.

- ID: CVE-2017-2171. Vulnerabilidad en un complemento de Zendesk en las secuencias de comandos entre sitios, permitía a los atacantes ejecutar código remoto. La solución fue actualizar el complemento.
- ID: CVE-2017-18542. Existía un complemento llamado 'zendesk-help-center' para WordPress el cual permitía a atacantes realizar ataques XSS. La vulnerabilidad se solucionó con actualizaciones y bugfix.

5. **Citrix**.

   - ID: CVE-2022-27512. Consiste en la interrupción temporal del servicio de licencias ADM de la aplicación la cual provoca un control inadecuado de un recurso. La solución fue lanzar versiones nuevas.
   - ID: CVE-2022-27503. Vulnerabilidad la cual permite ejecutar secuencias de comandos entre sitios (XSS), es decir, permitía a los atacantes realizar ataques XSS. La solución fue aplicar parches y lanzar nuevas versiones.
   - ID: CVE-2022-26355. Vulnerabilidad que hace que las implementaciones configuradas para almacenar certificados de seguridad, almacenen incorrectamente dicha clave del proveedor, problema que solo ocurre cuando se usa PowerShell. Citrix actualizó los servicios de autenticación y nuevas versiones.

6. **Cisco WebEx**.

   - ID: CVE-2022-20863. En la interfaz de usuario de Cisco WebEx existía una vulnerabilidad en la cual un atacante podía manipular el contenido que había dentro de la interfaz, esto porque la aplicación no representaba correctamente los caracteres. No hay soluciones alternativas para esta vulnerabilidad.
   - ID: CVE-2022-20852. Esta vulnerabilidad se dió en su interfaz web, consistía en que un atacante podía inyectar un script malicioso (XSS) dentro de la página. Cisco ha lanzado actualizaciones para dicha vulnerabilidad aunque no hay soluciones alternativas.
   - ID: CVE-2022-20778. Existía una vulnerabilidad en la autenticación de Cisco Webex Meetings en la cual un atacante podía realizar ataques XSS contra un usuario. Cisco ha lanzado actualizaciones para dicha vulnerabilidad aunque no hay soluciones alternativas.

7. **Google Workspace**.
   Las siguientes vulnerabilidades son de todos los productos de Google Cloud lo cual incluye a Google Workspace.

   - ID: CVE-2022-39278. Vulnerabilidad la cual provoca un error en el procesamiento de solicitudes lo que le permite a los atacantes enviar un mensaje que provoca el bloqueo del plano de control. No hay soluciones alternativas para esta vulnerabilidad sólo se recomienda trabajar en versiones anteriores.
   - ID: CVE-2022-1941. Vulnerabilidad en el análisis de mensajes y administración de memoria en implementaciones de C++ y Python el cual puede terminar en una falta de memoria al procesar mensajes y provocar denegación del servicio en los servicios que utilizan bibliotecas. Se está solucionando mediante actualizaciones en las versiones de algunos paquetes.
   - ID: CVE-2022-2327. En el kernel de Linux se puede realizar una escalada en cuanto a los privilegios locales la cual permite a un usuario sin privilegios realizar un root. No hay soluciones alternativas para esta vulnerabilidad, sólo se han lanzado parches.

Referencias.

- El concepto de CVE. (s/f). Redhat.com. Recuperado el 6 de octubre de 2022, de https://www.redhat.com/es/topics/security/what-is-cve
- Tú reportas, ellos actúan. (2018, mayo 17). INCIBE-CERT. https://www.incibe-cert.es/blog/tu-reportas-ellos-actuan
- Tes. (2021, agosto 12). Todo sobre CWE: enumeración de debilidades comunes. Parasoft. https://es.parasoft.com/blog/what-is-cwe
- CVSS versión 3, ¿cómo cambia la evaluación de vulnerabilidades? (2015, junio 25). WeLiveSecurity. https://www.welivesecurity.com/la-es/2015/06/25/cvss-version-3/
- Cve - cve. (s/f). Mitre.org. Recuperado el 6 de octubre de 2022, de https://cve.mitre.org/index.html