Alerta de Seguridad

Riesgo de vulnerabilidades IT y OT

Julio-2023

Sobre Axus

Axus es una empresa líder en ciberseguridad, con presencia en el Perú y Latinoamérica. Asesora a clientes en la protección de su información e infraestructura tanto en ámbitos industriales (OT) como en ámbitos corporativos (IT) y viene registrando una creciente participación en el ámbito de Internet de las Cosas (IoT) y en la protección de entornos Cloud e Híbridos.

En base a su reputación como especialista con los principales fabricantes de la industria y su equipo profesional en permanente capacitación, Axus genera valor a través de una visión consultiva que busca definir soluciones a la medida de las necesidades de cada cliente.

Alertas de Ciberseguridad

A continuación, compartimos con ustedes algunas de las alertas más relevantes de marzo.

Alertas de Seguridad IT:

- StackRot: vulnerabilidad crítica en Linux kernel 6.1
- Multiple Vulnerabilities in CloudPak for Watson AIOps
- Vulnerabilidad crítica “Follina” es explotada activamente mediante documentos de Office
- Microsoft: un ataque DDoS causó la caída de Outlook y OneDrive a principios de junio

Alertas de Seguridad OT/ICS:

- CosmicEnergy un malware ICS que no debe ser ignorado
- Cl0p Ransomware usando MOVEit atacó Siemens Energy y Schneider Electric

StackRot: vulnerabilidad crítica en Linux kernel 6.1

Tipo de Ataque: Vulnerabilidad

Medio de Propagación: Internet

1. PRODUCTOS AFECTADOS:

- Linux kernel 6.1 a 6.4

2. RESUMEN:

StackRot es una vulnerabilidad que afecta al subsistema de administración de memoria del kernel de Linux, que es responsable de implementar la memoria virtual, la paginación de demanda y la asignación de memoria para los programas del kernel y del espacio de usuario.

3. DETALLE:

La vulnerabilidad StackRot (CVE-2023-3269) fue descubierta e informada por el investigador de seguridad Ruihan Li. Se origina en el manejo de la expansión de la pila dentro del subsistema de administración de memoria del kernel. Específicamente, el punto débil se encuentra en el Maple Tree, un nuevo sistema de estructura de datos para la administración de áreas de memoria virtual (VMA) introducido en el kernel 6.1 de Linux. Este árbol se basa en el mecanismo de lectura-copia-actualización (RCU por sus siglas en inglés) y reemplazó a los Red-Black Tree.

La vulnerabilidad se aprovecha de un problema de uso después de liberar (UAF por sus siglas en inglés), que ocurre cuando el árbol reemplaza un nodo sin obtener el bloqueo de escritura de administración de memoria (MM).

4. RECOMENDACIONES:

Para mitigar el riesgo de la vulnerabilidad StackRot, se recomienda a los usuarios verificar la versión del kernel de Linux que están utilizando en su distribución. Si están utilizando una versión afectada, deben **actualizar a una versión más reciente** que contenga el parche de seguridad. Se destaca que no todas las distribuciones principales de Linux han adoptado la versión 6.1 del kernel, por lo que se debe verificar si la distribución utilizada es vulnerable.

5. REFERENCIAS:

- https://www.bleepingcomputer.com/news/security/new-stackrot-linux-kernel-flaw-allows-privilege-escalation/
- https://github.com/lrh2000/StackRot

Múltiples Vulnerabilidades en CloudPak para Watson AIOps

Tipo de Ataque: Vulnerabilidades

Medio de Propagación: Internet

1. PRODUCTOS AFECTADOS:

- IBM Cloud Pak for Watson AIOps

2. RESUMEN:

Cloud Pak for AIOps es un software de inteligencia artificial aplicada a la gestión de Operaciones de TI para remediación y gestión de incidentes. Se han identificado múltiples vulnerabilidades críticas que permiten el escalamiento de privilegios, ejecución de código arbitrario, evasión de restricciones de seguridad, entre otras.

3. DETALLE:

Se han solucionado múltiples vulnerabilidades en IBM Cloud Pak for Watson AIOps versión 4.1. Las vulnerabilidades corregidas incluyen:

- CVE-2021-37219: Se encontró una vulnerabilidad en HashiCorp Consul y Consul Enterprise que permite a un atacante remoto obtener privilegios elevados en el sistema. Esto se debió a un defecto en la capa Raft RPC. El atacante puede enviar una solicitud especialmente diseñada utilizando agentes no servidores con un certificado válido firmado por la misma CA para obtener privilegios elevados y acceder a funciones exclusivas del servidor.
- CVE-2023-32314: Se descubrió una vulnerabilidad en el módulo Node.js vm2 que permite a un atacante remoto ejecutar código arbitrario en el sistema. Esto se debió a una falla de escape en el sandbox. El atacante puede enviar una solicitud especialmente diseñada para ejecutar código arbitrario en el sistema.
- CVE-2023-32313: Se encontró una vulnerabilidad en el módulo Node.js vm2 que permite a un atacante remoto evadir restricciones de seguridad. Esto se debió a un defecto en el método de inspección de nodos. El atacante puede enviar una solicitud especialmente diseñada para editar opciones para console.log.
- CVE-2023-24536: Golang Go es vulnerable a un ataque de denegación de servicio debido a un defecto durante el análisis de formularios multipartes. Un atacante remoto puede enviar una entrada especialmente diseñada para consumir grandes cantidades de CPU y memoria, lo que resulta en una condición de denegación de servicio.
- CVE-2023-24537: Golang Go era vulnerable a un ataque de denegación de servicio debido a un bucle infinito causado por un desbordamiento de enteros al llamar a cualquiera de las funciones de análisis. Un atacante remoto puede enviar una entrada especialmente diseñada para provocar una condición de denegación de servicio.
- CVE-2023-24538: Golang Go permite a un atacante remoto ejecutar código arbitrario en el sistema debido a que no se consideraban correctamente las comillas invertidas (`) como delimitadores de cadena de JavaScript. Un atacante puede enviar una solicitud especialmente diseñada para ejecutar código arbitrario en el sistema.

RECOMENDACIONES:

Se recomienda a los usuarios abordar estas vulnerabilidades instalando las correcciones proporcionadas por IBM. No se han proporcionado soluciones alternativas ni mitigaciones.

REFERENCIAS:

- https://www.ibm.com/products/cloud-pak-for-aiops
- https://www.ibm.com/support/pages/node/7009745

Vulnerabilidad crítica “Follina” es explotada activamente mediante documentos de Office

Tipo de Ataque: **Explotación de vulnerabilidades**

Medio de Propagación: **Internet**

1. **PRODUCTOS AFECTADOS:**

- Aplicaciones Office

2. **RESUMEN:**

La vulnerabilidad zero-day llamada Follina ha sido explotada activamente a través de documentos de Microsoft Office. Esta vulnerabilidad crítica permite a los atacantes ejecutar comandos maliciosos de forma remota al abrir un documento de Office. La vulnerabilidad, registrada como CVE-2022-30190, se encuentra en Microsoft Support Diagnostic Tool (MSDT) y permite la ejecución remota de código cuando se llama a MSDT utilizando el protocolo de URL desde una aplicación como Word.

3. **DETALLE:**

Los atacantes que aprovechan esta vulnerabilidad pueden ejecutar código arbitrario a través de PowerShell, con los privilegios de la aplicación que realiza la llamada. Esto les permite instalar programas maliciosos, eliminar o modificar datos y crear nuevas cuentas con los privilegios del usuario.

La vulnerabilidad Follina no requiere la inserción de código malicioso en las macros de un documento, lo que la hace aún más peligrosa. Los investigadores han descubierto muestras de documentos maliciosos que explotan esta vulnerabilidad desde mayo. También se han encontrado campañas de phishing que distribuyen malware, como Qbot, aprovechando esta vulnerabilidad.

4. **RECOMENDACIÓN:**

Dado que la vulnerabilidad Follina sigue siendo explotada activamente, es importante que los usuarios realicen la actualización del sistema y estén atentos a futuras actualizaciones y parches que puedan ser lanzados por Microsoft.

5. **REFERENCIAS:**

- https://www.welivesecurity.com/la-es/2022/06/08/follina-vulnerabilidad-critica-explotada-mediante-documentos-office/
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-30190

Microsoft: un ataque DDoS causó la caída de Outlook y OneDrive a principios de junio

Tipo de Ataque: DDoS

Medio de Propagación: Internet

1. **PRODUCTOS AFECTADOS:**

- Outlook y OneDrive

2. **RESUMEN:**

Microsoft ha confirmado que el grupo de ciberdelincuentes conocido como Storm-1359 (Anonymous Sudan) fue responsable de los ataques de denegación de servicio distribuido (DDoS) que causaron interrupciones en sus servicios, incluyendo Outlook y OneDrive, a principios de junio. Un ataque DDoS busca colapsar un sitio web o recurso de red inundándolo con tráfico malicioso para que no pueda funcionar correctamente.

3. **DETALLE:**

Microsoft detectó aumentos repentinos en el tráfico de algunos de sus servicios y abrió una investigación para rastrear la actividad DDoS llevada a cabo por el grupo Storm-1359, también conocido como Anonymous Sudan. Este grupo se enfoca en grandes organizaciones y agencias gubernamentales y se opone a las políticas de Sudán, aunque algunos investigadores los vinculan con Rusia.

Según el análisis de Microsoft, Storm-1359 tiene acceso a una colección de botnets y herramientas que le permiten lanzar ataques DDoS desde múltiples servicios, infraestructuras de proxy abiertas y desde la nube. Su objetivo es propagar publicidad y interrumpir los servicios de Microsoft, agotando los recursos del sistema con una gran carga de protocolos de enlace SSL/TLS y procesamiento de solicitudes HTTPS. También emplean un ataque llamado "Slowris" que mantiene abierta la conexión y el recurso solicitado en la memoria del servidor web.

Como medida de protección, Microsoft recomienda utilizar Azure Web Application Firewall (WAF) para proteger las aplicaciones web y crear reglas personalizadas para bloquear y clasificar automáticamente los ataques HTTP y HTTPS.

4. **RECOMENDACIÓN:**

Este incidente destaca la importancia de contar con medidas de seguridad adecuadas, como firewalls y reglas personalizadas, para proteger los servicios en línea contra ataques DDoS y garantizar su disponibilidad y funcionamiento normal.

5. **REFERENCIAS:**

- https://elcomercio.pe/tecnologia/ciberseguridad/microsoft-asegura-que-un-ataque-ddos-causo-la-caida-de-outlook-y-onedrive-a-principios-de-junio-ciberseguridad-noticia/
- Recent Teams, Office outages were caused by cyberattacks: Microsoft | Computerworld

CosmicEnergy un malware ICS que no debe ser ignorado

Tipo de Ataque: Malware

Medio de Propagación: Internet

1. PRODUCTOS AFECTADOS:

- Sistemas de control industriales

2. RESUMEN:

El malware para sistemas de control industrial (ICS) llamado CosmicEnergy, vinculado a Rusia, no representa una amenaza inmediata para la tecnología operativa (OT) debido a sus errores y falta de madurez, según la firma de ciberseguridad industrial Dragos. El malware fue descubierto recientemente y está diseñado para apuntar a sistemas de control industrial utilizados en la transmisión y distribución eléctrica. Aunque no representa una amenaza inmediata, Dragos advierte a las organizaciones que no deben ignorarlo.

3. DETALLE:

El malware CosmicEnergy consta de dos componentes principales: LightWork, que implementa el protocolo de comunicación IEC104 para modificar el estado de las Unidades Terminales Remotas (RTU) de encendido/apagado, y PieHop, que se conecta a un servidor remoto MS SQL para cargar archivos y enviar comandos remotos a una RTU utilizando LightWork.

Dragos ha analizado CosmicEnergy y ha determinado que no posee las capacidades de ataque completas de otros malwares ICS, como Industroyer e Industroyer2, que se utilizaron para atacar el sector energético de Ucrania. Además, no hay evidencia de que el malware haya sido desplegado en la naturaleza. Parece haber sido creado para escenarios de entrenamiento y contiene parámetros codificados de manera rígida para un rango específico de equipos.

Aunque CosmicEnergy no representa una amenaza inmediata, Dragos recomienda a las organizaciones industriales tomar medidas para proteger sus sistemas contra posibles ataques con este tipo de malware. Esto incluye restringir el acceso y monitorear los servidores MS SQL.

4. RECOMENDACIONES

La existencia de CosmicEnergy debe llevar a las organizaciones a revisar y ajustar las reglas y configuraciones de su firewall, así como asegurarse de tener visibilidad de los protocolos ICS que atraviesan su red.

5. REFERENCIAS:

- https://hub.dragos.com/hubfs/116-Whitepapers/Dragos_SB_COSMICENERGY_June23_FINAL_WEB.pdf?hsLang=en
- https://www.securityweek.com/cosmicenergy-ics-malware-poses-no-immediate-threat-but-should-not-be-ignored/

Cl0p Ransomware usando MOVEit atacó Siemens Energy y Schneider Electric

Medio de Propagación: Red, Internet

1. **PRODUCTOS AFECTADOS:**
   - Sistemas de información
2. **RESUMEN:**

MOVEit es un producto de software de transferencia de archivos gestionado producido por Ipswitch, Inc. (ahora parte de Progress Software). MOVEit encripta archivos y utiliza protocolos de transferencia de archivos seguros para transferir datos, además de proporcionar servicios de automatización y análisis.

3. **DETALLE:**

El 31 de mayo de 2023, Progress Software informó una vulnerabilidad de inyección SQL en MOVEit. Dicha vulnerabilidad permite a un atacante acceder a la base de datos de MOVEit Transfer desde su aplicación web sin autenticarse. El 15 de junio se hizo pública otra vulnerabilidad que podría dar lugar a un acceso no autorizado.

Las empresas Schneider Electric y Siemens Energy han confirmado que han sido atacados por un grupo llamados Cl0p ransomware, dicho grupo explotó la vulnerabilidad en el software de transferencia de archivos administrados (MFT) MOVEit, logrando acceder a mucha información y posteriormente a negociar con empresas que fueron afectadas.

La vulnerabilidad ha sido identificada con el código CVE-2023-34362 y ya cuenta con parches disponibles para su mitigación.

4. **RECOMENDACIONES**

Actualizar el software MOVEit con los últimos parches de seguridad publicados.

5. **REFERENCIAS:**
   - https://www.securityweek.com/siemens-energy-schneider-electric-targeted-by-ransomware-group-in-moveit-attack/
   - https://www.securityweek.com/ransomware-group-used-moveit-exploit-to-steal-data-from-dozens-of-organizations/