GammaCSOC-CERT
By Gamma Ingenieros

GAMMA INGENIEROS

Boletín de Ciberseguridad Semanal

Edición º1925

BOLETÍN DE CIBERSEGURIDAD SEMANAL

Bienvenido a su boletín semanal de ciberseguridad generado por Gamma Ingenieros. A través de esta publicación tenemos el propósito de compartir contenidos relevantes para nuestras operaciones y aliados de negocio.

Aquí encontrará información sobre vulnerabilidades, alertas tempranas, noticias del sector, incidentes de ciberseguridad, tecnologías y servicios relacionados, entre otros.

VISTA RÁPIDA

	CRÍTICO	URGENTE	IMPORTANTE
VULNERABIILIDADES	4	0	0
MALWARE	1	0	0
NOTICIAS DE CIBERSEGURIDAD	0	0	1

VULNERABILIDADES

Alerta: Vulnerabilidad crítica en Cisco IOS XE permite secuestro total de dispositivos (CVE-2025-20188)

Cisco ha corregido una vulnerabilidad de máxima gravedad en su sistema operativo IOS XE, específicamente en los controladores de LAN inalámbrica. La falla, identificada como CVE-2025-20188, permite a atacantes remotos no autenticados ejecutar comandos arbitrarios con privilegios de nivel root, comprometiendo completamente el dispositivo afectado.

La vulnerabilidad reside en la gestión de tokens web JSON (JWT) en la interfaz de administración basada en web. Al explotar esta falla, un atacante puede obtener acceso total al sistema, lo que representa un riesgo crítico para la seguridad de la red

.

Los CVE relacionados a este compromiso de seguridad son:

- CVE-2025-20188

Recomendaciones de mitigación:

- Actualizar el software IOS XE a la versión más reciente proporcionada por Cisco que corrige esta vulnerabilidad.
- Restringir el acceso a la interfaz de administración web desde redes no confiables mediante listas de control de acceso (ACLs) y firewalls.
- Implementar autenticación multifactor (MFA) para acceder a la interfaz de administración.
- Monitorear los registros del sistema en busca de actividades inusuales que puedan indicar intentos de explotación.

Prioridad: Critica.

Ampliar Información:

- https://blog.segu-info.com.ar/2025/05/cisco-corrige-una-falla-de-maxima.html

Alerta: Cuatro vulnerabilidades críticas en servicios cloud de Microsoft — una con CVSS 10/10

Microsoft ha corregido cuatro vulnerabilidades críticas en sus servicios cloud, específicamente en Azure y Power Apps. La más grave, identificada como CVE-2025-29813, obtuvo una puntuación CVSS de 10/10, permitiendo a atacantes con acceso mínimo obtener control persistente sobre proyectos en Azure DevOps. Las otras tres vulnerabilidades también presentan riesgos significativos, con puntuaciones CVSS de 9.9 y 9.1, afectando a Azure Automation, Azure Storage Resource Provider y Microsoft Power Apps

Los CVE relacionados a este compromiso de seguridad son**:**

- CVE-2025-29813 (CVSS 10.0): Azure DevOps — Gestión inadecuada de tokens de pipeline que permite escalada de privilegios y control persistente
- CVE-2025-29827 (CVSS 9.9): Azure Automation — Fallo de autorización que permite a usuarios autenticados elevar sus permisos en entornos compartidos
- CVE-2025-29972 (CVSS 9.9): Azure Storage Resource Provider — Vulnerabilidad SSRF que permite suplantar peticiones internas y acceder a datos no autorizados.
- CVE-2025-47733 (CVSS 9.1): Microsoft Power Apps — Vulnerabilidad SSRF sin autenticación previa que permite exfiltración de datos mediante peticiones manipuladas.

Recomendaciones de mitigación:

- Revisar registros de actividad: Analizar logs de pipelines, runbooks y almacenamiento en busca de actividades inusuales, como tokens reutilizados o peticiones internas sospechosas.
- Aplicar el principio de mínimo privilegio: Limitar los permisos de identidades, service principals y suscripciones de Azure para reducir la superficie de ataque.
- Segregar entornos: Separar los entornos de desarrollo y producción para evitar que un acceso limitado comprometa recursos sensibles.
- Monitorear con herramientas de seguridad: Utilizar soluciones como Defender for Cloud o SIEM para detectar actividades anómalas relacionadas con SSRF y uso indebido de tokens.

Prioridad: Critica.

Ampliar Información:

- https://unaaldia.hispasec.com/2025/05/microsoft-corrige-cuatro-fallos-criticos-en-sus-servicios-cloud-uno-alcanza-la-maxima-gravedad-10-10.html
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2025-29813
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2025-29827
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2025-29972
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2025-47733

Alerta: SAP publica 16 parches de seguridad en mayo de 2025, incluyendo una vulnerabilidad crítica activamente explotada (CVE-2025-31324)

El 13 de mayo de 2025, SAP lanzó su boletín mensual de seguridad, abordando 16 nuevas vulnerabilidades en sus productos, de las cuales una es de severidad crítica, cuatro de alta y once de severidad media. La vulnerabilidad crítica, identificada como CVE-2025-31324, está siendo activamente explotada y afecta al componente Visual Composer de SAP NetWeaver

Los CVE relacionados a este compromiso de seguridad son**:**

- CVE-2025-31324 (CVSS 10.0)

Recomendaciones de mitigación:

- Aplicar las actualizaciones de seguridad proporcionadas por SAP: Especialmente la Nota de Seguridad 3604119, que aborda la raíz de la vulnerabilidad CVE-2025-31324.
- Revisar y deshabilitar componentes innecesarios: Si Visual Composer no es utilizado, considerar su desactivación para reducir la superficie de ataque.
- Monitorear los sistemas SAP: Buscar indicadores de compromiso, como cargas de archivos no autorizadas o actividad inusual en el sistema.
- Implementar controles de acceso estrictos: Asegurar que solo usuarios autorizados tengan acceso a componentes críticos del sistema.

Prioridad: Critica.

Ampliar Información:

- https://support.sap.com/en/my-support/knowledge-base/security-notes-news/may-2025.html
- https://onapsis.com/blog/active-exploitation-of-sap-vulnerability-cve-2025-31324/

- https://www.incibe.es/incibe-cert/alerta-temprana/avisos/actualizacion-de-seguridad-de-sap-de-mayo-de-2025

Alerta: Vulnerabilidad crítica en Optigo ONS NC600 permite ejecución remota de comandos vía credenciales codificadas (CVE-2025-4041)

Se ha identificado una vulnerabilidad crítica en los dispositivos ONS NC600 de Optigo Networks, específicamente en las versiones 4.2.1-084 hasta 4.7.2-330. La falla, catalogada como CVE-2025-4041, permite a un atacante remoto no autenticado conectarse al servidor SSH del dispositivo utilizando credenciales codificadas, lo que posibilita la ejecución de comandos arbitrarios en el sistema operativo

Los CVE relacionados a este compromiso de seguridad son**:**

- CVE-2025-4041

Recomendaciones de mitigación:

- Actualizar el firmware del dispositivo: Aplicar las actualizaciones proporcionadas por Optigo Networks que corrigen esta vulnerabilidad.
- Implementar medidas de seguridad adicionales:
    - Utilizar una tarjeta de red dedicada (NIC) en el equipo BMS y destinar esta máquina exclusivamente para gestionar la configuración de red OT mediante OneView.
    - Configurar reglas en el firewall del enrutador que solo permitan el acceso a OneView a dispositivos previamente autorizados.
    - Asegurar el acceso a OneView utilizando una conexión VPN confiable.
- Limitar la exposición de la red: Asegurar que los dispositivos de control no sean accesibles desde internet y estén aislados de las redes empresariales.
- Monitorear los sistemas: Revisar los registros de actividad en busca de accesos no autorizados o comportamientos inusuales.

Prioridad: Critica.

Ampliar Información:

- https://www.cisa.gov/news-events/ics-advisories/icsa-25-126-01
- https://nvd.nist.gov/vuln/detail/CVE-2025-4041

Recomendaciones generales sobre vulnerabilidades:

Para mitigar las vulnerabilidades en los sistemas, se recomiendan las siguientes medidas claves.

1. Aplicar las actualizaciones de seguridad proporcionadas por Microsoft para las versiones afectadas de Windows Serve
2. Instalar regularmente parches de seguridad para corregir vulnerabilidades conocidas.
3. Añadir una capa extra de protección para dificultar el acceso no autorizado por medio de 2FA.
4. Minimizar los permisos de usuarios y aplicaciones para reducir riesgos.
5. Implementar actualizaciones gradualmente, con capacidad de revertir cambios en caso de errores.
6. Usar herramientas de detección de intrusiones para identificar actividades sospechosas.

MALWARE

Alerta Crítica: Grupos BianLian y RansomExx explotan vulnerabilidad en SAP NetWeaver para desplegar malware avanzado

El 14 de mayo de 2025, se confirmó que los grupos cibercriminales BianLian y RansomExx están explotando activamente la vulnerabilidad crítica CVE-2025-31324 en SAP NetWeaver Visual Composer. Esta falla permite la carga de archivos sin autenticación, facilitando la ejecución remota de código y el compromiso total del sistema afectado

Los CVE relacionados a este compromiso de seguridad son**:**

- CVE-2025-31324 (CVSS 10.0): Permite a atacantes no autenticados cargar archivos arbitrarios en SAP NetWeaver Visual Composer, resultando en ejecución remota de código.
- CVE-2025-42999 (CVSS 9.1): Vulnerabilidad de deserialización en el mismo componente, explotada en conjunto con CVE-2025-31324 para mantener persistencia en el sistema.
- CVE-2025-29824: Falla de escalada de privilegios en el sistema de archivos de registro común de Windows (CLFS), utilizada por los atacantes para obtener privilegios elevados en sistemas comprometidos.

Tácticas observadas:

- Despliegue de malware PipeMagic: Trojan modular utilizado para establecer control sobre el sistema comprometido.
- Uso de Brute Ratel C2: Framework de comando y control avanzado desplegado mediante ejecución de tareas MSBuild inline, facilitando la comunicación con servidores de los atacantes.
- Persistencia mediante webshells: Instalación de shells web tras la explotación inicial para mantener acceso continuo al sistema.

Recomendaciones para mitigar el riesgo:

- Aplicar parches de seguridad de SAP: Implementar las notas de seguridad 3594142 (CVE-2025-31324) y 3604119 (CVE-2025-42999) para corregir las vulnerabilidades identificadas.
- Revisar y eliminar webshells: Inspeccionar los sistemas en busca de shells web instaladas y eliminarlas para prevenir accesos no autorizados.
- Actualizar sistemas Windows: Asegurar que los sistemas operativos Windows estén actualizados para mitigar la explotación de CVE-2025-29824.

- Monitorear actividad sospechosa: Implementar herramientas de detección para identificar comportamientos anómalos y posibles compromisos en los sistemas.
- Revisar configuraciones de seguridad: Asegurar que las configuraciones de SAP y otros sistemas críticos sigan las mejores prácticas de seguridad para reducir la superficie de ataque.

Prioridad: Critica.

Ampliar Información:

- https://thehackernews.com/2025/05/bianlian-and-ransomexx-exploit-sap.html
- https://onapsis.com/blog/active-exploitation-of-sap-vulnerability-cve-2025-31324/

Recomendaciones generales sobre malware:

Para protegerse contra malware, es esencial:

1. Actualizar el software y sistemas operativos regularmente, ya que los atacantes suelen explotar vulnerabilidades en software desactualizado.
2. Usar antivirus y herramientas antimalware confiables, manteniéndolos siempre al día.
3. Habilitar la autenticación multifactor (MFA) para proteger cuentas sensibles.
4. Evitar correos electrónicos y enlaces sospechosos, ya que el phishing es una de las principales vías de propagación de malware.
5. Realizar copias de seguridad regulares de archivos importantes para protegerse contra pérdidas en caso de ataques como el ransomware.
6. Limitar los privilegios de usuario, evitando el uso innecesario de cuentas con permisos de administrador.

NOTICIAS DE CIBERSEGURIDAD

Análisis: Redes "IPv6 Mostly" — Transición estratégica hacia IPv6 con soporte para IPv4

El blog de LACNIC presenta el concepto de Redes Mayormente IPv6 (IPv6 Mostly Networks) como una estrategia efectiva para facilitar la transición de IPv4 a IPv6. Estas redes implementan tecnologías como NAT64 y DNS64, permitiendo que dispositivos con soporte exclusivo para IPv6 accedan a servicios IPv4 sin necesidad de direcciones IPv4 propias

Resumen técnico:

Definición: Según el RFC 8925, una red "IPv6 Mostly" proporciona servicios NAT64 (posiblemente con DNS64) y conectividad IPv4, permitiendo la coexistencia de hosts solo IPv6, de doble pila y solo IPv4 en el mismo segmento.

Ventajas:

- Reducción en la necesidad de direcciones IPv4, mitigando el impacto del agotamiento de estas direcciones.
- Facilita una transición gradual hacia IPv6, permitiendo a los operadores desactivar IPv4 en los hosts finales de manera progresiva.
- Mejora la eficiencia de la red al reducir la sobrecarga de cabecera y optimizar el enrutamiento

Consideraciones:

- Es esencial una planificación cuidadosa para garantizar la compatibilidad de aplicaciones y servicios durante la transición.
- La implementación de NAT64 y DNS64 requiere una configuración adecuada para evitar problemas de conectividad.

Recomendaciones para organizaciones:

- Evaluar la infraestructura actual: Determinar la capacidad de los dispositivos y servicios para soportar IPv6 y planificar las actualizaciones necesarias.
- Implementar NAT64 y DNS64: Configurar estos servicios para permitir que dispositivos IPv6 accedan a recursos IPv4 sin requerir direcciones IPv4 individuales.
- Capacitación del personal: Asegurar que el equipo técnico esté familiarizado con las tecnologías y mejores prácticas relacionadas con IPv6.
- Monitoreo y pruebas continuas: Realizar pruebas periódicas para garantizar la funcionalidad y rendimiento de la red durante y después de la transición.

Prioridad: Importante.

Ampliar Información:

https://blog.lacnic.net/ipv6-mostly-network/