GammaCSOC-CERT
By Gamma Ingenieros

GAMMA INGENIEROS

Boletín de Ciberseguridad Semanal

Edición º2325

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	5	0	0
NOTICIAS DE CIBERSEGURIDAD	0	1	0

VULNERABILIDADES

Inyección de comando local en FortiManager y FortiAnalyzer (FG-IR-23-167)

Fortinet ha publicado el aviso de seguridad FG-IR-23-167 advirtiendo sobre una vulnerabilidad de inyección de comandos (CWE-78) identificada como CVE-2023-42788, que permite a atacantes con acceso local ejecutar comandos arbitrarios con privilegios del servicio CLI.

CVE: CVE-2023-42788

Impacto potencial:

Un atacante local con pocos privilegios puede manipular argumentos del CLI para inyectar y ejecutar comandos arbitrarios en FortiManager y FortiAnalyzer (versiones 6.2.0–7.4.0).

Recomendaciones de mitigación:

- Actualizar sistemas a la última versión que incluya el parche de Fortinet.
- Restringir el acceso local solo a personal administradores de confianza.

- Monitorear actividad de CLI para detectar comandos inusuales.
- Aplicar principio de mínimo privilegio en las cuentas y servicios gestionados.

Prioridad: Crítica.

Ampliar Información:

- https://www.fortiguard.com/psirt/FG-IR-23-167
- https://www.cybersecurity-help.cz/vdb/SB2023101257
- https://nvd.nist.gov/vuln/detail/CVE-2023-42788
- https://www.doxnet.com/article.cfm?ArticleNumber=7712

Vulnerabilidades en VMWARE NSX, Cloud Foundation y Telco Cloud

El 4 de junio de 2025, VMware emitió el aviso de seguridad VMSA-2025-0012, corrigiendo tres vulnerabilidades de Stored Cross-Site Scripting (XSS) que afectan a VMware NSX, Cloud Foundation y Telco Cloud Platform. Estas fallas permiten la inyección de scripts persistentes en interfaces administrativas y de red.

Resumen técnico:

VMware identificó fallos en diversos componentes de red y gestión que afectan a sus plataformas de virtualización y redes definidas por software (SDN), incluyendo:

- VMware NSX: Múltiples vulnerabilidades críticas en el plano de control y la interfaz de usuario web, que podrían permitir inyección de comandos y escalada de privilegios.
- Cloud Foundation: Fallos que permiten a atacantes ganar acceso no autorizado, comprometiendo la seguridad de entornos VMware gestionados como servicio integral.
- Telco Cloud Platform: Vulnerabilidades en componentes de orquestación y telecomunicaciones, que podrían exponer datos de tráfico o comprometer la disponibilidad de servicios de red.

- CVE-2025-22243 – XSS en NSX Manager UI (CVSS 7.5): Permite a atacantes con privilegios inyectar scripts al modificar configuraciones de red que se ejecutan cuando el administrador view la interfaz.
- CVE-2025-22244 – XSS en gateway firewall (CVSS 6.9): Permite inyección de código en páginas de filtrado que se muestran a usuarios al bloquear sitios.
- CVE-2025-22245 – XSS en configuración de router ports (CVSS 5.9): Permite a atacantes con permisos modificar descripciones de puertos para inyectar código que se ejecuta al visualizar las configuraciones.

Productos y versiones afectados:

- VMware NSX 4.0.x, 4.1.x, 4.2.x
- VMware Cloud Foundation 5.0.x – 5.2.x (requiere patch asíncrono de NSX)
- VMware Telco Cloud Infrastructure 2.x – 3.x
- VMware Telco Cloud Platform 3.x – 5.x

Impacto potencial:

- Ejecución remota de código en servidores host o máquinas virtuales.
- Escalada de privilegios en componentes de red y gestión.
- Intercepción de tráfico entre VMs o servicios.
- Posible interrupción de servicios críticos en entornos de telecomunicaciones y nube

Recomendaciones de mitigación:

- Aplicar los parches de seguridad disponibles de VMware para NSX, Cloud Foundation y Telco Cloud Platform.
  - NSX 4.2.x → 4.2.2.1
  - NSX 4.2.1.x → 4.2.1.4
  - NSX 4.1.x / 4.0.x → 4.1.2.6
- Revisar registros del sistema para detectar actividad sospechosa o intentos de explotación.

- Limitar el acceso administrativo a estos entornos solo a personal de confianza.
- Monitorear y segmentar redes virtuales, especialmente en infraestructura Telco, para contener posibles compromisos.

Prioridad: Crítica.

Ampliar Información:

- https://ciberseguridad.euskadi.eus/noticia/2025/vulnerabilidades-en-vmware-nsx-cloud-foundation-y-telco-cloud/webcyb00-contcibglos/es/
- https://www.isssource.com/vmware-clears-multiple-nsx-vulnerabilities
- https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/25738
- https://gbhackers.com/vmware-nsx-xss-vulnerability
- https://www.picussecurity.com/resource/blog/vmware-cloud-foundation-cve-2021-39144-vulnerability-exploitation-explained
- https://cybersecuritynews.com/vmware-nsx-xss-vulnerability

Vulnerabilidades críticas en Cisco ISE, IMC Y NDFC

Cisco ha lanzado actualizaciones de seguridad importantes para abordar tres vulnerabilidades críticas: una en Identity Services Engine (ISE) en la nube, otra en Integrated Management Controller (IMC) y una más en Nexus Dashboard Fabric Controller (NDFC). Todas estas fallas permiten acceso no autorizado o manipulación de sistemas.

Resumen técnico:

- CVE-2025-20286(CVSS 9.9):
  Afecta a ISE ejecutado en AWS, Azure y OCI. El instalador genera credenciales estáticas compartidas entre instancias, permitiendo a un atacante no autenticado con una credencial de una instalación comprometer otras. Existe código PoC público.

- CVE-2025-20261(CVSS 8.8):
  Falla en el proceso SSH del IMC de servidores UCS B/C/S/X. Permite a un atacante autenticado (con credenciales débiles o comprometidas) acceder a servicios internos y elevar privilegios.
- CVE-2025-20163(CVSS 8.7):
  Vulnerabilidad en la validación de host key SSH de NDFC. Permite un ataque "man-in-the-middle" que intercepta conexiones SSH y roba credenciales

Impacto potencial:

- Acceso administrativo completo en ISE multi-nube.
- Control interno del servidor UCS via IMC.
- Secuestro de sesión SSH y robo de credenciales en entornos gestionados por NDFC.

Recomendaciones de mitigación:

- Aplicar actualizaciones y hotfixes inmediatamente:
  - ISE (nube): usar hotfixes para versiones 3.1–3.4.
  - IMC y NDFC: actualizar firmware desde Cisco.
- Restringir el acceso administrativo (SSH y web) a personal de confianza y redes seguras.
- Rotar credenciales y revisar accesos: especialmente en ISE una vez aplicado el parche.
- Monitorear logs y tráfico: para detectar actividad inusual en SSH y accesos a ISE.
- Seguir recomendaciones del CERT local/infraestructura: como uso de ACLs en entornos cloud.

Prioridad: Crítica.

Ampliar Información:

- https://sevenice.net/vulnerabilidad-severa-en-cisco-ise-en-funcionamiento-a-traves-de-servicios-en-la-nube

- https://www.securityweek.com/cisco-patches-critical-ise-vulnerability-with-public-poc/
- https://unaaldia.hispasec.com/2025/06/cisco-corrige-vulnerabilidad-critica-en-ise-con-poc-publica.html
- https://www.cert.gov.py/vulnerabilidades-en-los-productos-cisco/

Vulnerabilidades críticas en Apache Tomcat impactan componentes de HPE

Se han identificado dos vulnerabilidades críticas en Apache Tomcat utilizadas en productos de HPE, incluyendo servidores y appliances que integran Tomcat como contenedor web. Estas fallas permiten ejecución remota de código (RCE) o exposición de información sensible, colocando en riesgo entornos empresariales gestionados por HPE

Resumen técnico:

Las fallas residen en componentes centrales del motor Catalina de Tomcat, usados en productos HPE que dependen de esta plataforma Java. Aunque no se especifican los CVE, las vulnerabilidades permiten:

- Inyección de comandos o gadgets de RCE a través de peticiones HTTP manipuladas.
- Lectura arbitraria de archivos confidenciales en el sistema del servidor.

Las versiones afectadas incluyen builds recientes utilizadas en HPE y otros entornos Java basados en Tomcat.

Impacto potencial:

- Ejecución remota de código con privilegios del servidor.
- Acceso a archivos del sistema, como credenciales, claves o configuraciones.
- Riesgo extendido a múltiples clientes si se usan appliances compartidos o configuraciones estándar.

Recomendaciones de mitigación:

- Actualizar Apache Tomcat a la versión parcheada tan pronto estén disponibles los paquetes oficiales.
- Aplicar las actualizaciones de firmware/software que HPE publique para sus productos basados en Tomcat.
- Restringir el acceso a interfaces HTTP expuestas utilizando firewalls y network ACLs.
- Monitorear los registros de Tomcat y del sistema operativo para detectar patrones de explotación, como peticiones anómalas o actividad inusual.
- Auditar y endurecer la configuración de Tomcat en productos HPE: desactivar el WAR deployment automático, restringir directorios web y aplicar políticas de seguridad.

Prioridad: Crítica.

Ampliar Información:

- https://ciberseguridad.euskadi.eus/noticia/2025/vulnerabilidades-en-apache-tomcat-con-impacto-en-software-de-hpe/webcyb00-contcibglos/es/
- https://ciberseguridad.euskadi.eus/contenidos/enlace/cyb_guia_20250609/es_def/adjuntos/Avisos-Tecnicos-hasta-el-9-de-junio.pdf

Más de 20 riesgos de configuración en Salesforce Industry Cloud, incluidas cinco vulnerabilidades CVE

Investigadores de AppOmni han descubierto más de 20 configuraciones inseguras en las plataformas de Salesforce Industry Cloud, entre ellas cinco vulnerabilidades formalmente registradas como CVE. Aunque algunas han sido corregidas por Salesforce, otras requieren acciones específicas por parte de los clientes

Resumen técnico:

- CVE-2025-43697: Permite extraer datos cifrados de campos sin que se haya aplicado correctamente la política de Field-Level Security (FLS).
- CVE-2025-43698: Bypass de controles FLS mediante consultas SOQL.

- CVE-2025-43699: FlexCard no valida correctamente los permisos de acceso (CVSS:5.3).
- CVE-2025-43700: FlexCard permite visualizar datos cifrados sin restricciones (CVSS:7.5).
- CVE-2025-43701: Usuarios invitados pueden consultar configuraciones personalizadas no protegidas.

Salesforce corrigió tres de estas fallas del lado del servidor, pero al menos dos requieren intervención manual en la configuración de cada instancia de cliente. Además, se detectaron 15 configuraciones adicionales que podrían permitir filtración de datos sensibles, robo de sesión, exposición de lógica de negocio e incluso credenciales.

Impacto potencial:

- Acceso a información confidencial de clientes o empleados.
- Robo de sesiones activas o claves API.
- Alteración de flujos de negocio construidos sobre plataformas low-code.
- Riesgo elevado de ataques automatizados sobre instancias mal configuradas

Recomendaciones de mitigación:

- Activar la opción EnforceDMFLSAndDataEncryption en la instancia de Salesforce, que impone el uso de FLS y la protección de datos cifrados.
- Revisar y endurecer las configuraciones en módulos como FlexCards, Data Mappers, Integration Procedures (IProcs) y OmniScripts.
- Ejecutar análisis con herramientas como AppOmni o equivalentes para identificar configuraciones riesgosas.
- Implementar monitoreo continuo sobre accesos a objetos sensibles y registros de actividad.
- Capacitar a los administradores de Salesforce sobre prácticas seguras en entornos low-code/no-code.

Prioridad: Crítica.

Ampliar Información:

- https://thehackernews.com/2025/06/researchers-uncover-20-configuration.html

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.

NOTICIAS DE CIBERSEGURIDAD

Microsoft corrige fallos de autenticación en Windows Server causados por actualizaciones de abril 2025

Microsoft ha solucionado problemas que afectaban la autenticación en controladores de dominio Windows Server 2016, 2019, 2022 y 2025, provocados por la actualización KB5055523 de abril de 2025.

Resumen técnico:

- Las actualizaciones de abril introdujeron una validación más estricta mediante el parámetro msds-KeyCredentialLink usado con la autenticación Kerberos PKINIT / certificado en Active Directory.
- En controladores de dominio, esto causó errores en el procesamiento de inicios de sesión Kerberos, Windows Hello for Business y delegación basada en certificados.
- Esto fue consecuencia de un parche para CVE-2025-26647, que estableció nuevos controles de certificado. Posteriormente los logs comenzaron a registrar eventos 45 y 21 indicando rechazos de certificados

Impacto potencial:

- Fallos en autenticación de usuarios y dispositivos (Kerberos, smart cards, SSO).
- Interrupciones en entornos corporativos, afectando VPNs, RDP, servicios de directorio y acceso a recursos.
- Eventos excesivos en logs Event IDs 45 (advertencias) y 21 (errores) tras el arranque.

Recomendaciones para mitigar el riesgo:

- Instalar las actualizaciones correctivas de junio 2025:
  - KB5060842 (Server 2025)
  - KB5060526 (Server 2022)
  - KB5060531 (Server 2019)
  - KB5061010(Server2016)

  Esto corrige los problemas de autenticación reportados.
- Si aún no puede aplicar el parche, ajuste el registro:
  - HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Kdc
  - AllowNtAuthPolicyBypass = 1

  Esto restaura el comportamiento anterior y evita rechazos por bypass. Evita el valor 2, que bloquea autenticación con certificados.

- Monitorear eventos 45 y 21 en registros de Controladores de Dominio para validar estabilidad tras actualización.
- Verificar autenticación de Smart Card y WHfB en entornos certificados.
- Planificar actualizaciones automatizadas mediante WSUS o Intune para evitar futuros incidentes de este tipo.

Prioridad: Urgente.

Ampliar Información:

- https://www.heise.de/en/news/Windows-Server-2025-AD-login-problems-after-installing-the-April-updates-10378360.html
- https://learn.microsoft.com/en-us/windows/release-health/status-windows-server-2025
- https://www.bleepingcomputer.com/news/microsoft/microsoft-fixes-windows-server-auth-issues-caused-by-april-updates/