PERÚ | Presidencia del Consejo de Ministros | Secretaría de Gobierno y Transformación Digital

ALERTA INTEGRADA DE SEGURIDAD DIGITAL

Asociación de Bancos del Perú

ALERTA INTEGRADA DE SEGURIDAD DIGITAL

116-2025-CNSD

La presente **Alerta Integrada de Seguridad Digital** corresponde a un análisis técnico periódico realizado por el Comando Conjunto de las Fuerzas Armadas, el Ejército del Perú, la Marina de Guerra del Perú, la Fuerza Aéreadel Perú, la Dirección Nacional de Inteligencia, la Policía Nacional del Perú, la Asociación de Bancos del Perú y el Centro Nacional de Seguridad Digital de la Secretaría de Gobierno y Transformación Digital de la Presidencia del Consejo de Ministros, en el marco de la Seguridad Digital del Estado Peruano.

El objetivo de esta alerta **es informar a los responsables de la seguridad digital de las entidades públicas y lasempresas privadas sobre las amenazas en el entorno digital** para advertir las situaciones que pudieran afectar la continuidad de sus servicios en favor de la población.

Las marcas y logotipos de empresas privadas y/o entidades públicas se reflejan para ilustrar la información que los ciudadanos reciben por redes sociales u otros medios y que atentan contra la confianza digital de las personas y de las mismas empresas **de acuerdo con lo establecido por el Decreto de Urgencia 007-2020**.

La presente Alerta Integrada de Seguridad Digital es información netamente especializada para informar a las áreas técnicas de entidades y empresas.

Contenido

La Nueva Herramienta 'Defendnot' Engaña a Windows para Desactivar Microsoft Defender 4
Vulnerabilidad en el sistema operativo Junos de Juniper Networks 6
Múltiples vulnerabilidades de severidad crítica en Mozilla Firefox 7
Vulnerabilidad en Gardener External DNS Management 8
Múltiples vulnerabilidades en Dell PowerScale InsightIQ 9
Índice alfabético 10

Centro Nacional de Seguridad Digital	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°116	Fecha: 19-05-2025
		Página: 4 de 10

Componente que reporta	CENTRO NACIONAL DE SEGURIDAD DIGITAL		
Nombre de la alerta	La Nueva Herramienta 'Defendnot' Engaña a Windows para Desactivar Microsoft Defender		
Tipo de Ataque	RootKit	Abreviatura	RootKit
Medios de propagación	USB, Disco, Red, Correo, Navegación de Internet		
Código de familia	C	Código de Sub familia	C03
Clasificación temática familia	Código Malicioso		

Descripción

1. ANTECEDENTES:

En el diverso y siempre cambiante paisaje de la seguridad digital, una nueva herramienta llamada Defendnot ha causado revuelo, al engañar a los sistemas operativos Windows para desactivar automáticamente Microsoft Defender.

Microsoft Defender es el antivirus que viene en el sistema operativo Windows. Es muy buena opción para detectar y eliminar amenazas. Por ello, los piratas informáticos pueden utilizar diferentes estrategias para que deje de funcionar con normalidad y así actuar sin restricciones en el sistema.

2. DETALLES:

Defendnot explota una funcionalidad poco documentada del Windows Security Center (WSC) API, diseñada originalmente para que los antivirus de terceros se registren como proveedores de seguridad en el sistema. Cuando Windows detecta un antivirus registrado correctamente, desactiva automáticamente Microsoft Defender para evitar conflictos entre múltiples motores de protección.

El creador de la herramienta, el investigador conocido como es3n1n, logró desarrollar una versión desde cero que evita problemas legales de herramientas previas como no-defender, que fue retirado de GitHub bajo presiones legales, tras una solicitud DMCA por parte de un proveedor antivirus cuyo código se usó sin autorización.

Para eludir los requisitos habituales del API (como la protección Protected Process Light (PPL) y firmas digitales válidas), Defendnot inyecta una DLL en el proceso Taskmgr.exe, una aplicación firmada y confiable por Microsoft. Desde este contexto privilegiado, la herramienta registra un "antivirus falso" con un nombre visual personalizado, logrando así desactivar Defender de inmediato.

Una vez registrado, el sistema queda sin protección activa si no hay otro antivirus legítimo instalado.

Algunas características y consideraciones:

- En cuanto a persistencia, utiliza el Programador de tareas de Windows para ejecutarse en cada inicio de sesión.

- Es decir, esta herramienta se puede configurar para que se ejecute siempre al iniciar Windows, por lo que siempre estaría bloqueando el funcionamiento normal de Microsoft Defender. Ese equipo, por tanto, estaría totalmente desprotegido ante posibles ataques.
- Permite definir el nombre del antivirus falso, habilitar/deshabilitar el registro y activar un modo de registro detallado usando un loader configurable ctx.bin.

Si bien es cierto, Defendnot fue presentado como un proyecto de investigación, su publicación pone en evidencia cómo APIs legítimas y procesos confiables pueden ser manipulados para ser utilizados como vectores de ataque y desactivar protecciones esenciales sin levantar alertas inmediatas.

Actualmente, Microsoft Defender detecta y bloquea a Defendnot como Win32/Sabsik.FL.!ml, pero este tipo de ataques revela la importancia de reforzar las protecciones del sistema operativo.

3. RECOMENDACIONES:

- Considerar usar un antivirus complementario.
- Verificar regularmente el estado de Microsoft Defender en endpoints, especialmente en entornos corporativos.
- Implementar soluciones de seguridad avanzadas, como sistemas de detección y respuesta de endpoints (EDR), con capacidades de detección de manipulación de API y procesos, y software de detección y prevención de intrusiones (IDS/IPS), para identificar y bloquear comportamientos sospechosos antes de que causen daños significativos.
- Restringir la ejecución de procesos no autorizados y monitorear anomalías en Task Scheduler.
- Mantener sistemas actualizados y reforzar el monitoreo de procesos confiables pero susceptibles de inyección.
- Utilizar contraseñas largas y complejas, y diferentes para cada plataforma.
- Evitar abrir archivos adjuntos o enlaces sospechosos en correos electrónicos no solicitados o mensajes de redes sociales.
- Habilitar la autenticación de dos factores en toda aplicación que esté disponible.
- Educar a los usuarios sobre las amenazas más recurrentes, y cómo reconocer los intentos de phishing.

Fuente de Información:	• hxxps://www.comprarantivirus.es/new-defendnot-tool-bypasses-microsoft-defender-descubre-como/ • hxxps://devel.group/blog/defendnot-la-nueva-herramienta-que-engana-a-windows-para-desactivar-microsoft-defender/ • hxxps://www.comprarantivirus.es/new-defendnot-tool-bypasses-microsoft-defender-descubre-como/

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°116	Fecha: 19-05-2025 Página: 6 de 10

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad en el sistema operativo Junos de Juniper Networks		
Tipo de Ataque	Explotación de vulnerabilidades conocidas	Abreviatura	EVC
Medios de propagación	Red, Internet		
Código de familia	H	Código de Sub familia	H01
Clasificación temática familia	Intento de intrusión		

Descripción

1. ANTECEDENTES:

Juniper Networks, Inc. ha publicado una vulnerabilidad de severidad **ALTA** de tipo manejo inadecuado de condiciones excepcionales en el Demonio de Clase de Servicio (cosd) que afecta al sistema operativo Junos. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante autenticado basado en red con privilegios bajos provoque una denegación de servicio (DoS) limitada.

2. DETALLES:

La vulnerabilidad de severidad **alta** identificada por MITRE como CVE-2024-21610 de tipo manejo inadecuado de condiciones excepcionales en el Demonio de Clase de Servicio (cosd) de Juniper Networks Junos OS, podría permitir a un atacante autenticado basado en red con privilegios bajos provoque una denegación de servicio (DoS) limitada.

En un escenario de CoS escalado con miles de interfaces, cuando cosd gestiona comandos específicos con privilegios bajos, recibidos a través de NETCONF, SSH o Telnet, en nombre de mgd, los procesos secundarios del demonio de administración (mgd) se bloquean. En caso de Netconf a través de SSH, esto provoca el bloqueo de sesiones SSH, de modo que, al alcanzar el límite de conexiones SSH, ya no se pueden establecer nuevas sesiones. Se observará un comportamiento similar para Telnet, etc.

A. Productos afectados:

- Versiones de Junos OS anteriores a 20.4R3-S9.
- Versiones del sistema operativo Junos anteriores a 21.2R3-S7.
- Versiones del sistema operativo Junos anteriores a 21.3R3-S5.
- Versiones del sistema operativo Junos anteriores a 21.4R3-S5.
- Versiones del sistema operativo Junos anteriores a 22.1R3-S4.
- Versiones del sistema operativo Junos anteriores a 22.2R3-S3.
- Versiones del sistema operativo Junos anteriores a 22.3R3-S2.
- Versiones del sistema operativo Junos anteriores a 22.4R3.
- Versiones de Junos OS anteriores a 23.2R1-S2.
- Versiones del sistema operativo Junos anteriores a 23.2R2.
- Versiones del sistema operativo Junos anteriores a 23.4R1.

3. RECOMENDACIONES:

- Actualizar las siguientes versiones de software para resolver este problema específico: Junos OS: 20.4R3-S9, 21.2R3-S7, 21.3R3-S5, 21.4R3-S5, 22.1R3-S4, 22.2R3-S3, 22.3R3-S2, 22.4R3, 23.2R1-S2, 23.2R2, 23.4R1 y todas las versiones posteriores.
- Monitorear la cantidad de procesos mgd bloqueados y, una vez que alcanzan un nivel alto, se pueden finalizar de manera proactiva.

Fuente de Información:	• hxxps://supportportal.juniper.net/s/article/2024-04-Security-Bulletin-Junos-OS-MX-Series-In-a-scaled-subscriber-scenario-if-CoS-information-is-gathered-mgd-processes-gets-stuck-CVE-2024-21610?language=en_US • hxxps://prsearch.juniper.net/problemreport/PR1757003 • hxxp://supportportal.juniper.net/JSA75751

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°116	Fecha: 19-05-2025 Página: 7 de 10

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Múltiples vulnerabilidades de severidad crítica en Mozilla Firefox		
Tipo de Ataque	Explotación de vulnerabilidades conocidas	Abreviatura	EVC
Medios de propagación	Red, Internet		
Código de familia	H	Código de Sub familia	H01
Clasificación temática familia	Intento de intrusión		

Descripción

1. ANTECEDENTES:

Fundación Mozilla ha publicado dos vulnerabilidades de severidad **CRÍTICA** de día cero de tipo acceso fuera de límites al resolver objetos “Promise” de JavaScript y acceso fuera de límites al optimizar sumas lineales en su navegador Firefox. La explotación exitosa de estas vulnerabilidades podría permitir a un atacante remoto no autenticado acceder a información confidencial y la ejecución de código.

2. DETALLES:

La vulnerabilidad de severidad **crítica** identificada por MITRE como CVE-2025-4918 de tipo acceso fuera de límites, podría permitir a un atacante realizar una lectura o escritura fuera de los límites en un objeto "Promise" de JavaScript.

La vulnerabilidad de severidad **crítica** identificada por MITRE como CVE-2025-4919 de tipo acceso fuera de límites, podría permitir a un atacante realizar una lectura o escritura fuera de los límites en un objeto JavaScript al confundir el tamaño del índice de la matriz.

A. Productos afectados:

- Todas las versiones de Firefox anteriores a la 138.0.4 (incluido Firefox para Android).
- Todas las versiones de Firefox Extended Support Release (ESR) anteriores a la 128.10.1.
- Todas las versiones de Firefox ESR anteriores a 115.23.1.

3. RECOMENDACIÓN:

- Actualizar los productos afectados a la última versión de software disponible que abordan estas vulnerabilidades.

Fuente de Información:	• hxxps://bugzilla.mozilla.org/show_bug.cgi?id=1966612 • hxxps://www.mozilla.org/security/advisories/mfsa2025-36/ • hxxps://www.mozilla.org/security/advisories/mfsa2025-37/ • hxxps://www.mozilla.org/security/advisories/mfsa2025-38/

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°116	Fecha: 19-05-2025
		Página: 8 de 10

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad en Gardener External DNS Management		
Tipo de Ataque	Explotación de vulnerabilidades conocidas	Abreviatura	EVC
Medios de propagación	Red, Internet		
Código de familia	H	Código de Sub familia	H01
Clasificación temática familia	Intento de intrusión		

Descripción

1. ANTECEDENTES:

GitHub, Inc. ha publicado una vulnerabilidad de severidad **CRÍTICA** de tipo validación de entrada incorrecta que afecta a Gardener External DNS Management, una herramienta utilizada para gestionar entradas DNS externas en clústeres de Kubernetes, comúnmente utilizados en entornos nativos de la nube y DevOps. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto no autenticado comprometer los sistemas afectados, lo que podría conducir a un acceso no autorizado o la interrupción de las operaciones de administración de DNS.

2. DETALLES:

La vulnerabilidad de severidad **crítica** identificada por MITRE como CVE-2025-47282 de tipo validación de entrada incorrecta que afecta a Gardener External DNS Management, podría permitir a un atacante remoto no autenticado comprometer los sistemas afectados, lo que podría conducir a un acceso no autorizado o la interrupción de las operaciones de administración de DNS.

Esta vulnerabilidad afecta a todas las instalaciones de Gardener, independientemente del proveedor de nube pública utilizado para los clústeres de clusters/shoot. El componente afectado es `gardener/external-dns-management`. El componente `external-dns-management` también puede implementarse en las semillas mediante la extensión `gardener/gardener-extension-shoot-dns-service` cuando esta está habilitada. En este caso, todas las versiones de la extensión `shoot-dns-service` <= v1.60.0` se ven afectadas por esta vulnerabilidad.

Un atacante con privilegios administrativos de bajo nivel podría escalar su acceso y obtener el control total del clúster de semillas. Esto podría provocar un acceso no autorizado a la infraestructura del clúster, posible vulnerabilidad de los sistemas de gestión del clúster, capacidad para manipular o apropiarse de los recursos del clúster.

La explotación exitosa puede dar como resultado que los atacantes obtengan control sobre las entradas DNS administradas por el sistema de administración de DNS externo de Gardener, que podrían aprovecharse para futuros ataques, como redirigir el tráfico o interrumpir los servicios.

No hay evidencia de que exista una prueba de concepto pública. Actualmente, no hay evidencia de explotación.

A. Productos afectados:

- Gardener External DNS Management, versiones anteriores a 0.23.6.

3. RECOMENDACIONES:

- Actualizar el producto afectado a la última versión de software disponible que aborda esta vulnerabilidad.
- Actualizar gardener-extension-shoot-dns-service a una versión superior a v1.60.0.3.
- Monitorear la actividad del DNS para detectar cambios inusuales o modificaciones no autorizadas, ya que podrían indicar intentos de explotación.
- Restringir el acceso a las interfaces de administración de DNS y asegúrese de que solo el personal autorizado pueda realizar cambios.
- Implementar controles de acceso estrictos y el principio del mínimo privilegio.
- Realizar una auditoría de seguridad exhaustiva de las configuraciones de clúster existentes.

Fuente de Información:	• hxxps://github.com/gardener/external-dns-management/security/advisories/GHSA-xwgg-m7fx-83wx

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°116	Fecha: 19-05-2025
		Página: 9 de 10

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Múltiples vulnerabilidades en Dell PowerScale InsightIQ		
Tipo de Ataque	Explotación de vulnerabilidades conocidas	Abreviatura	EVC
Medios de propagación	Red, Internet		
Código de familia	H	Código de Sub familia	H01
Clasificación temática familia	Intento de intrusión		

Descripción

1. ANTECEDENTES:

La empresa Dell Technologies ha publicado dos vulnerabilidades de severidad **ALTA** de tipo gestión inadecuada de privilegios y agotamiento de los recursos que afecta a varios de sus productos. La explotación exitosa de estas vulnerabilidades podría permitir a un atacante remoto no autenticado ejecutar código arbitrario en el sistema y realizar un ataque de denegación de servicio (DoS).

2. DETALLES:

La vulnerabilidad de severidad **alta** identificada por MITRE como CVE-2025-30475 de tipo gestión inadecuada de privilegios, podría a un atacante remoto comprometer el sistema afectado. La vulnerabilidad existe debido a una gestión inadecuada de privilegios. Un atacante remoto no autenticado puede ejecutar código arbitrario en el sistema.

La vulnerabilidad de severidad **media** identificada por MITRE como CVE-2025-30476 de tipo agotamiento de recursos, podría permitir a un atacante remoto realizar un ataque de DoS. La vulnerabilidad existe porque la aplicación no controla adecuadamente el consumo de recursos internos. Un atacante remoto puede provocar el agotamiento de recursos y realizar un ataque de denegación de servicio DoS.

A. Productos afectados:

- PowerScale InsightIQ Scale: 5.0.0 - 5.2.0.
- PowerScale InsightIQ Simple: 5.0.0 - 5.2.0.

3. RECOMENDACIÓN:

- Actualizar los productos afectados a la última versión de software disponible que abordan estas vulnerabilidades.

Fuente de Información:	• hxxps://www.dell.com/support/kbdoc/en-us/000317889/dsa-2025-186-security-update-for-dell-powerscale-inightiq-multiple-security-vulnerabilities

Índice alfabético

Explotación de vulnerabilidades conocidas 6, 7, 8, 9
RootKit 4