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

135-2025-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

Centro Nacional de Seguridad Digital	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°135	Fecha: 11-06-2025
		Página: 4 de 8

Componente que reporta	CENTRO NACIONAL DE SEGURIDAD DIGITAL		
Nombre de la alerta	Nueva falla de Secure Boot permite a los atacantes instalar malware bootkit		
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:

Investigadores de seguridad han revelado una nueva omisión de Arranque Seguro (Secure Boot), que afecta a casi todos los sistemas que confían en el certificado "UEFI CA 2011" de Microsoft, es decir, prácticamente todo el hardware compatible con Arranque Seguro.

2. DETALLES:

El investigador de Binarly, Alex Matrosov, ha revelado un nuevo bypass en el arranque seguro y que puede usarse para desactivar la seguridad en PC y servidores e instalar malware Bootkit. El investigador descubrió el defecto, identificado como CVE-2025-3052, después de encontrar una utilidad de actualización de BIOS firmada con el certificado de firma UEFI de Microsoft.

La utilidad fue diseñada originalmente para tabletas resistentes, pero como se firmó con el certificado UEFI de Microsoft, puede ejecutarse en cualquier sistema seguro habilitado para arranque.

Esta utilidad lee una variable NVRAM de usuarios (ihisiparambuffer) sin validarla. Si un atacante tiene derechos de administración a un sistema operativo, puede modificar esta variable para que los datos arbitrarios se escriban en ubicaciones de memoria durante el proceso de arranque UEFI. Esto se hace antes de que se cargue el sistema operativo, o incluso el núcleo.

Aprovechando esta vulnerabilidad, Binarly creó un exploit de prueba de concepto para anular la variable global gSecurity2, que se utiliza para aplicar el Arranque Seguro. “Para nuestra prueba de concepto (PoC), elegimos sobrescribir la variable global gSecurity2”, explica el informe de Binarly.

Esta variable contiene un puntero al protocolo de arquitectura Security2, que la función LoadImage utiliza para implementar el Arranque Seguro. Al establecerla en cero, desactivamos el Arranque Seguro, lo que permite la ejecución de cualquier módulo UEFI sin firmar.

Una vez deshabilitado, los atacantes pueden instalar malware bootkit que puede ocultarse del sistema operativo y desactivar otras funciones de seguridad.

Investigaciones adicionales descubrieron que el módulo vulnerable había estado circulando desde al menos finales de 2022 y luego subió a Virustotal en 2024, donde lo vio binarly, el cual reveló el defecto a CERT/CC el 26 de febrero de 2025, con CVE-2025-3052, que se mitigó como parte del parche de Microsoft Junio 2025.

Sin embargo, durante este proceso, Microsoft determinó que la falla impactó otros 13 módulos, que se agregaron a la base de datos de revocación, de tal manera que el DBX actualizado lanzado durante el parche el martes 10 de junio de 2025 contiene 14 hash nuevos.

3. RECOMENDACIÓN:

- Instalar el archivo dbx actualizado inmediatamente a través de las actualizaciones de seguridad para proteger sus dispositivos, ya que Microsoft ha añadido los hashes del módulo afectado a la lista de revocación de dbx de Secure Boot.

Fuente de Información:	• hxxps://blog.segu-info.com.ar/2025/06/nueva-falla-de-secure-boot-permite-los.html • hxxps://www.bleepingcomputer.com/news/security/new-secure-boot-flaw-lets-attackers-install-bootkit-malware-patch-now/

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°135	Fecha: 11-06-2025
		Página: 5 de 8

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidades de severidad crítica en productos Microsoft		
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:

Microsoft Corporation ha publicado dos vulnerabilidades de severidad **CRÍTICA** de tipo control externo del nombre o ruta de archivo e inyección de comando que afecta a varios de sus productos. La explotación exitosa de estas vulnerabilidades podría permitir a un atacante remoto no autenticado la ejecución remota de código y divulgación de información a través de una red.

2. DETALLES:

WebDAV es un conjunto de extensiones del protocolo HTTP que permite a los usuarios crear, editar, mover y administrar archivos de forma colaborativa directamente en servidores web, transformando la web de un medio de solo lectura a una plataforma colaborativa con capacidad de escritura. Está definido por RFC 4918 y fue desarrollado por el Grupo de Trabajo de Ingeniería de Internet (IETF) para abordar la necesidad de autoría distribuida en la web.

La vulnerabilidad de severidad **alta** identificada por MITRE como CVE-2025-33053 de tipo control externo del nombre o ruta de archivo en WebDAV (Web Distributed Authoring and Versioning) de Microsoft Windows, podría permitir a un atacante no autorizado ejecutar código a través de una red explotando el control externo del nombre o ruta del archivo. La vulnerabilidad requiere la interacción del usuario (como hacer clic en una URL especialmente diseñada) y puede explotarse en toda la red con baja complejidad.

La vulnerabilidad se está explotando activamente en la naturaleza y se añadió a la lista de vulnerabilidades explotadas conocidas de la Agencia de Seguridad de Ciberseguridad e Infraestructura (CISA) de EE. UU. Esta vulnerabilidad es explotada activamente por el grupo de amenazas persistentes avanzadas (APT) Stealth Falcon mediante un archivo .url para ejecutar malware desde un servidor WebDAV controlado.

La vulnerabilidad de severidad **crítica** identificada por MITRE como CVE-2025-32711 de tipo inyección de comando en Microsoft 365 Copilot, podría permitir a un atacante no autorizado ejecutar comandos y divulgar información confidencial a través de una red sin requerir la interacción del usuario. No hay evidencia de que exista una prueba de concepto pública. Actualmente, no hay evidencia de explotación.

A. Productos afectados:

- La vulnerabilidad CVE-2025-33053 afecta a todas las versiones compatibles de Microsoft Windows.
- La vulnerabilidad CVE-2025-32711 afecta a Microsoft 365 Copilot.

3. RECOMENDACIÓN:

- Actualizar los productos afectados a la última versión de software disponible que abordan estas vulnerabilidades. Microsoft, a pesar de que WebDAV quedó obsoleto en 2023 y no está habilitado de forma predeterminada, lanzó parches en junio de 2025 tanto para las versiones nuevas como para algunas heredadas de Windows y Windows Server para abordar esta vulnerabilidad de día cero.

Fuente de Información:	• hxxps://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-33053 • hxxps://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-32711

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°135	Fecha: 11-06-2025
		Página: 6 de 8

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad en dispositivos Relion series 670, 650 y SAM600-IO de Hitachi Energy		
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:

Hitachi Energy ha publicado una vulnerabilidad de severidad **ALTA** de tipo discrepancia observable que afecta a varios de sus productos. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto no autenticado descifrar datos de la aplicación en tránsito.

2. DETALLES:

La vulnerabilidad de severidad **alta** identificada por MITRE como CVE-2022-4304 de tipo discrepancia observable, podría permitir a un atacante remoto no autenticado descifrar datos de la aplicación en tránsito.

Existe un canal lateral basado en tiempo en la implementación de descifrado RSA de OpenSSL, que podría ser suficiente para recuperar texto plano a través de una red en un ataque tipo Bleichenbacher. Para lograr un descifrado exitoso, un atacante tendría que enviar una gran cantidad de mensajes de prueba. La vulnerabilidad afecta a todos los modos de relleno RSA: PKCS#1 v1.5, RSA-OEAP y RSASVE.

Por ejemplo, en una conexión TLS, un cliente suele usar RSA para enviar un cifrado *pre-master secret* al servidor. Un atacante que hubiera observado una conexión genuina entre un cliente y un servidor podría usar esta falla para enviar mensajes de prueba al servidor y registrar el tiempo de procesamiento. Tras un número suficiente de mensajes, el atacante podría recuperar el *pre-master secret* utilizado para la conexión original y, por lo tanto, descifrar los datos de la aplicación enviados a través de ella.

A. Productos afectados:

- Relion 650: versión 2.2.0, versión 2.2.1.
- Relion 650: versiones 2.2.4.0 a 2.2.4.3.
- Relion 650: versiones 2.2.5.0 a 2.2.5.5.
- Relion 670: versión 2.2.0, versión 2.2.1.
- Relion 670: versiones 2.2.2.0 a 2.2.2.5.
- Relion 670: versiones 2.2.3.0 a 2.2.3.6.
- Relion 670: versiones 2.2.4.0 a 2.2.4.3.
- Relion 670: versiones 2.2.5.0 a 2.2.5.5.
- SAM600-IO: versión 2.2.1.
- SAM600-IO: versiones desde la 2.2.5.0 hasta la 2.2.5.5 (sin incluirla).

3. RECOMENDACIONES:

- Actualizar los productos afectados a la última versión de software disponible que abordan estas vulnerabilidades.
- Configurar los firewalls para proteger las redes de control de procesos de ataques que se originan desde fuera de la red.
- Proteger físicamente los sistemas de control de procesos contra el acceso directo de personal no autorizado.
- Evitar conectar directamente los sistemas de control a Internet.
- Separar las redes de control de procesos de otras redes a través de un sistema de firewall con puertos expuestos.
- No utilizar los sistemas de control de procesos para navegar por Internet, ni para enviar mensajes instantáneos ni para enviar correos electrónicos.
- Aplicar políticas y procesos de contraseñas adecuados.

Fuente de Información:	• hxxps://publisher.hitachienergy.com/preview?DocumentId=8DBD000157&languageCode=en&Preview=true • hxxps://www.cisa.gov/news-events/ics-advisories/icsa-25-160-02

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°135	Fecha: 11-06-2025
		Página: 7 de 8

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad de severidad crítica en la función auxiliar CryptHmacSign de la implementación de referencia TCG TPM2.0. de Intel		
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:

Se ha publicado una vulnerabilidad de severidad **CRÍTICA** de tipo lectura fuera de límites en la función auxiliar CryptHmacSign de la implementación de referencia TCG TPM2.0 de Intel. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante local autenticado con acceso a la interfaz TPM obtener acceso no autorizado a información confidencial y provocar una condición de denegación de servicio (DoS).

2. DETALLES:

La vulnerabilidad de severidad **crítica** identificada por MITRE como CVE-2025-2884 de tipo lectura fuera de límites en la función auxiliar CryptHmacSign de la implementación de referencia TCG TPM2.0, podría permitir a un atacante local autenticado con acceso a la interfaz TPM obtener acceso no autorizado a información confidencial y provocar una condición de denegación de servicio (DoS) del TPM. La vulnerabilidad se debe a una validación insuficiente del esquema de firma con respecto al algoritmo de la clave de firma, como se indica en la errata 1.83 del estándar TCG TPM2.0.

Un atacante con acceso a la interfaz de comandos TPM puede explotar esta vulnerabilidad enviando comandos especialmente diseñados. Esto puede provocar: acceso no autorizado a información confidencial de la memoria TPM y DoS del TPM, lo que podría afectar la seguridad del sistema.

Los atacantes locales autenticados con acceso a la interfaz TPM pueden explotar esta vulnerabilidad enviando comandos TPM creados maliciosamente. la lectura OOB puede permitir potencialmente la lectura de hasta 65.535 bytes más allá del búfer previsto, dependiendo del tamaño del búfer, lo que puede exponer material criptográfico sensible u otros datos confidenciales. la explotación también puede provocar que el TPM funcione mal o se bloquee, lo que resulta en la pérdida de servicios criptográficos.

Muchos de los principales proveedores (incluidos AMD, Qualcomm, Intel, Dell, Lenovo, Microsoft, etc.) aún no han proporcionado declaraciones públicas sobre su exposición a esta vulnerabilidad a junio de 2025.

A. Productos afectados:

- Implementaciones de TPM 2.0 basadas en el código de referencia TCG (rev. de especificación 01.83).

3. RECOMENDACIONES:

- Actualizar el producto afectado a la última versión de software disponible que aborda esta vulnerabilidad. Trusted Computing Group ha publicado una actualización de erratas (Errata 1.83) a la Especificación de la biblioteca TPM 2.0 y ha actualizado la implementación de referencia para abordar la vulnerabilidad.
- Monitorear los parches oficiales de Intel para los servicios de la plataforma de servidor.
- Revisar y actualizar las implementaciones de referencia de TPM2.0.
- Implementar la segmentación de red para limitar la superficie de ataque potencial.
- Realizar evaluaciones de seguridad exhaustivas de los sistemas relacionados con TPM.
- Restringir temporalmente el acceso a la red a los sistemas afectados si es posible.

Fuente de Información:	• hxxps://trustedcomputinggroup.org/about/security/ • hxxps://trustedcomputinggroup.org/wp-content/uploads/TPM2.0-Library-Spec-v1.83-Errata_v1_pub.pdf • hxxps://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-01209.html • hxxps://www.kb.cert.org/vuls/id/282450

Índice alfabético