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

083-2025-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°083	Fecha: 07-04-2025
		Página: 4 de 9

Componente que reporta	CENTRO NACIONAL DE SEGURIDAD DIGITAL		
Nombre de la alerta	NEPTUNE RAT ataca a usuarios de Windows y roba contraseñas de más de 270 aplicaciones		
Tipo de Ataque	Troyanos	Abreviatura	Troyanos
Medios de propagación	USB, Disco, Red, Correo, Navegación de Internet		
Código de familia	C	Código de Sub familia	C02
Clasificación temática familia	Código Malicioso		

Descripción

1. ANTECEDENTES:

Una reciente amenaza cibernética llamada Neptune RAT ha surgido como una preocupación creciente para los usuarios de Windows, apuntando a datos confidenciales y exhibiendo capacidades maliciosas avanzadas.

2. DETALLES:

Neptune RAT es un malware sofisticado desarrollado en Visual Basic .NET. Se distribuye en plataformas como GitHub, Telegram y YouTube, y suele promocionarse como el "RAT más avanzado".

El software está disponible sin código fuente, pero sus archivos ejecutables ofuscados dificultan el análisis para los expertos en ciberseguridad.

Neptune RAT v2 emplea comandos directos de PowerShell como:

- Invoke-RestMethod (irm): facilita la descarga de scripts maliciosos de Internet.
- Invoke-Expression (iex): ejecuta los scripts descargados.

Estos comandos permiten que el malware descargue y ejecute cargas codificadas alojadas en plataformas como catbox.moe, que se guardan en la carpeta AppData de la víctima para su ejecución.

Neptune RAT es un malware con múltiples funciones capaz de:

- Obtención de contraseñas en más de 270 aplicaciones, incluidos navegadores como Chrome, Opera y Brave.
- Funcionalidades del Crypto Clipper, alterando direcciones de billetera de criptomonedas en el portapapeles.
- Implementación de ransomware a través de módulos internos como Ransomware.dll.
- Monitoreo de escritorio en vivo para vigilancia de víctimas en tiempo real.
- Destrucción del sistema, incluida la reescritura del registro de arranque maestro (MBR).
- Desactivación del antivirus y manipulación del registro para persistencia.

El malware utiliza varios archivos DLL maliciosos para tareas específicas:

- Ransomware.dll cifra archivos y exige pagos en Bitcoin para descifrarlos.
- Chromium.dll roba contraseñas almacenadas en los perfiles del navegador.
- BlockAntivirus.dll desactiva las medidas de seguridad para evadir la detección.

Neptune RAT incorpora múltiples mecanismos de persistencia:

- Programador de tareas: crea tareas ocultas para ejecutar malware periódicamente.
- Modificación de claves de registro: agrega entradas a la clave Ejecutar en HKEY_CURRENT_USER para su ejecución automática al iniciar el sistema.

Además, la RAT emplea la detección de máquinas virtuales a través de consultas a la clase Win32_ComputerSystem.

Si el malware detecta entornos como VMware o VirtualBox, se desactiva para evitar que los investigadores de seguridad intercepten sus acciones.

Tras su ejecución, Neptune RAT manipula el sistema de la víctima mediante las siguientes acciones:

- Copiándose a sí mismo en la carpeta Roaming en AppData.
- Registrarse en la clave de ejecución del Registro de Windows para una infección sostenida.
- Automatizar tareas a través de la utilidad schtasks.exe para mantener una conexión continua con el servidor del atacante.

La carga útil del ransomware del malware, una vez lanzada, cifra todos los archivos accesibles y cambia sus extensiones a ".ENC".

A la víctima se le presentan instrucciones para el pago del rescate a través de un archivo de escritorio llamado "Cómo descifrar mis archivos.html".

El desarrollador de Neptune RAT comercializa activamente el malware a través de GitHub y sitios web personales, insinuando una versión paga más avanzada.

Neptune RAT es un malware muy potente con un arsenal de características que plantean riesgos importantes tanto para usuarios individuales como para organizaciones.

3. RECOMENDACIONES:

- Implementar soluciones robustas de protección de puntos finales y antimalware.
- Limitar el uso de comandos de PowerShell y monitoree solicitudes inusuales.
- Actualizar periódicamente los sistemas operativos y el software para mitigar las vulnerabilidades.
- Emplear estrategias proactivas de detección y monitoreo de amenazas.

Fuente de Información:	• hxxps://gbhackers.com/neptune-rat-targets-windows-users/

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°083	Fecha: 07-04-2025
		Página: 6 de 9

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Múltiples vulnerabilidades en el firmware BMC de la placa de servidor 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 múltiples vulnerabilidades de severidad **ALTA** de tipo exposición de información confidencial a un actor no autorizado, excepción no detectada, desbordamiento de búfer basado en montón y control de acceso inadecuado en el firmware BMC de la placa de servidor Intel. La explotación exitosa de estas vulnerabilidades podría permitir a un atacante remoto no autenticado obtener acceso a información confidencial, enumerar cuentas de usuario y realizar un ataque de denegación de servicio (DoS). Asimismo, un usuario local podría aumentar privilegios en el sistema de destino.

2. DETALLES:

La vulnerabilidad de severidad **crítica** identificada por MITRE como CVE-2023-25191 de tipo exposición de información confidencial a un actor no autorizado, podría permitir a un atacante remoto obtener acceso a información potencialmente confidencial. La vulnerabilidad existe debido a la excesiva salida de datos de Redfish en dispositivos AMI MegaRAC SPX. Un atacante remoto puede obtener una contraseña administrativa y comprometer el sistema afectado. Esta vulnerabilidad puede ser explotada por un atacante remoto no autenticado a través de la red local (LAN).

La vulnerabilidad de severidad **media** identificada por MITRE como CVE-2023-25192 de tipo exposición de información confidencial a un actor no autorizado, podría permitir enumerar cuentas de usuario. La vulnerabilidad existe debido a la excesiva salida de datos por parte de Redfish. Un atacante remoto puede enumerar cuentas de usuario. Esta vulnerabilidad puede ser explotada por un atacante remoto no autenticado a través de la red local.

La vulnerabilidad de severidad **media** identificada por MITRE como CVE-2025-20097 de tipo excepción no detectada, podría permitir realizar un ataque de DoS. La vulnerabilidad existe debido a una excepción no detectada en el firmware de OpenBMC. Un usuario remoto puede enviar una entrada especialmente diseñada al sistema y ejecutar un ataque de DoS.

La vulnerabilidad de severidad **baja** identificada por MITRE como CVE-2023-31276 de tipo desbordamiento de búfer basado en montón, podría permitir a un usuario local aumentar privilegios en el sistema. La vulnerabilidad existe debido a un error de límite. Un usuario local con privilegios puede provocar un desbordamiento de búfer basado en el montón y ejecutar código arbitrario con privilegios elevados. Esta vulnerabilidad puede explotarse localmente. El atacante debe tener credenciales de autenticación y autenticarse correctamente en el sistema.

La vulnerabilidad de severidad **baja** identificada por MITRE como CVE-2023-29164 de tipo control de acceso inadecuado, podría permitir a un usuario local aumentar privilegios en el sistema. La vulnerabilidad existe debido a restricciones de acceso indebidas en el firmware de BMC. Un usuario local puede escalar privilegios en el sistema.

A. Productos afectados:

- Intel Server Board M70KLP: anterior a 4.16.
- Intel Server Board M20NTP: anterior a 0027.D02.
- Intel Server Board M10JNP2SB: anterior a 7.220.
- Intel Server Board M50CYP y D50TNP: anterior a R01.01.0009.
- Intel Server Board S2600WF y S2600ST/BP: anterior al 02.01.0017.

3. RECOMENDACIÓN:

- Actualizar los productos afectados a la última versión de firmware disponible.

Fuente de Información:	• hxxps://9443417.fs1.hubspotusercontent-na1.net/hubfs/9443417/Security%20Advisories/AMI-SA-2023002.pdf • hxxps://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00990.html

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°083	Fecha: 07-04-2025 Página: 7 de 9

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

Cisco Systems, Inc. ha publicado dos vulnerabilidades de severidad **CRÍTICA** de tipo inserción de información confidencial en el archivo de registro y funcionalidad oculta que afecta a Cisco Smart Licensing Utility. La explotación exitosa de estas vulnerabilidades podría permitir a un atacante remoto no autenticado recopilar información confidencial o administrar servicios de Cisco Smart Licensing Utility en un sistema mientras el software se está ejecutando.

2. DETALLES:

La vulnerabilidad de severidad **crítica** identificada por MITRE como CVE-2024-20439 de tipo credenciales estáticas en Cisco Smart Licensing Utility, podría permitir que un atacante remoto no autenticado inicie sesión en un sistema afectado mediante el uso de una credencial administrativa estática. Esta vulnerabilidad se debe a una credencial de usuario estática no documentada para una cuenta administrativa. Un atacante podría explotar esta vulnerabilidad utilizando las credenciales estáticas para iniciar sesión en el sistema afectado. Una explotación exitosa podría permitir al atacante iniciar sesión en el sistema afectado con privilegios administrativos a través de la API de la aplicación Cisco Smart Licensing Utility.

La vulnerabilidad de severidad **crítica** identificada por MITRE como CVE-2024-20440 de tipo de divulgación de información en Cisco Smart Licensing Utility, podría permitir que un atacante remoto no autenticado acceda a información confidencial. Esta vulnerabilidad se debe a un exceso de verbosidad en un archivo de registro de depuración. Un atacante podría explotar esta vulnerabilidad enviando una solicitud HTTP manipulada a un dispositivo afectado. Una explotación exitosa podría permitir al atacante obtener archivos de registro que contienen información confidencial, incluyendo credenciales que permiten acceder a la API.

Las vulnerabilidades no dependen unas de otras. No es necesario explotar una vulnerabilidad para explotar la otra. Además, una versión de software afectada por una vulnerabilidad podría no verse afectada por la otra.

Nota: Estas vulnerabilidades no se pueden explotar a menos que un usuario haya iniciado Cisco Smart Licensing Utility y se encuentre en ejecución activa.

A. Productos afectados:

- Estas vulnerabilidades afectan a los sistemas si ejecutan una versión vulnerable de Cisco Smart Licensing Utility (versiones anteriores a 2.3.0), independientemente de la configuración del software.

3. RECOMENDACIÓN:

- Actualizar los paquetes afectados a la última versión disponible que Cisco ha lanzado para abordar esta vulnerabilidad. No existen soluciones alternativas.

Fuente de Información:	• hxxps://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cslu-7gHMzWmw

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°083	Fecha: 07-04-2025
		Página: 8 de 9

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Actualización de Red Hat Enterprise Linux 9 para Tomcat		
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 actualización que corrige dos vulnerabilidades de severidad **CRÍTICA** de tipo permisos, privilegios y controles de acceso, y validación de entrada incorrecta en Red Hat Enterprise Linux 9 para Tomcat. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto no autenticado la ejecución remota de código, obtener acceso a información confidencial y comprometer el sistema afectado.

2. DETALLES:

La vulnerabilidad de severidad **crítica** identificada por MITRE como CVE-2024-50379 de tipo permisos, privilegios y controles de acceso, podría permitir a un atacante remoto comprometer el sistema afectado. La vulnerabilidad existe debido a la falta de restricciones de acceso al servlet predeterminado. Si el servlet predeterminado tiene habilitada la escritura (el parámetro de inicialización de solo lectura se establece en un valor distinto al predeterminado, falso) para un sistema de archivos que no distingue entre mayúsculas y minúsculas, la lectura y carga simultáneas del mismo archivo bajo carga pueden eludir las comprobaciones de distinción entre mayúsculas y minúsculas de Tomcat y provocar que un archivo cargado se trate como un JSP, lo que conlleva la ejecución remota de código.

La vulnerabilidad de severidad **crítica** identificada por MITRE como CVE-2025-24813 de tipo validación de entrada incorrecta, podría permitir a un atacante remoto comprometer el sistema afectado. La vulnerabilidad existe debido a una validación insuficiente de la información proporcionada por el usuario al gestionar la carga de archivos mediante solicitudes HTTP PUT. Un atacante remoto puede enviar una solicitud HTTP PUT especialmente diseñada al servidor y obtener acceso a información confidencial o incluso ejecutar código arbitrario.

A. Productos afectados:

- Servidor Red Hat Enterprise Linux - AUS: 9.2.
- Red Hat Enterprise Linux para IBM z Systems: soporte de actualización ampliado: 9.2.
- Red Hat Enterprise Linux para Power, little endian: compatibilidad con actualizaciones extendidas: 9.2.
- Red Hat Enterprise Linux para ARM 64: compatibilidad con actualizaciones extendidas: 9.2.
- Red Hat Enterprise Linux Server para Power LE: Servicios de actualización para soluciones SAP: 9.2.
- Red Hat Enterprise Linux para x86_64 - Soporte de actualización extendido: 9.2.
- Tomcat (paquete Red Hat): anterior a 9.0.87-1.el9_2.3.

3. RECOMENDACIÓN:

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

Fuente de Información:	• hxxps://access.redhat.com/errata/RHSA-2025:3646

Índice alfabético