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

274-2024-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°274	Fecha: 27-11-2024
		Página: 4 de 8

Componente que reporta	CENTRO NACIONAL DE SEGURIDAD DIGITAL		
Nombre de la alerta	Hackeo a la Biblioteca Nacional del Perú afecta su cuenta de X con mensajes indeseados		
Tipo de Ataque	Acceso no autorizado a carpetas privadas		AccNoAutCarpPri
Medios de propagación	Red, Internet		
Código de familia	A	A	A01
Clasificación temática familia	Acceso no autorizado		

Descripción

1. **ANTECEDENTES:**

Desde el 22 de noviembre, la cuenta de la biblioteca ha sido utilizada para publicar contenido obsceno, lo que ha llevado a la institución a actuar rápidamente. En su comunicado, indicaron que están trabajando con especialistas en ciberseguridad para minimizar el impacto del ataque y proteger la información institucional.

2. **DETALLES:**

El 27 de noviembre, la Biblioteca Nacional del Perú emitió un comunicado en el que informó sobre el ataque cibernético, generando preocupación en la institución. Aseguraron que ya están tomando medidas para recuperar el control de la cuenta y evitar mayores daños.

Ante esta situación, la BNP solicitó a la comunidad no difundir ningún mensaje o publicación emitida desde la cuenta comprometida, ya que el acceso fue tomado por actores externos sin autorización.

El cambio en el nombre de usuario y perfil de la cuenta ha generado confusión, ya que existen otras cuentas en X que utilizan el nombre de la BNP. Sin embargo, la institución no ha anunciado planes para reemplazar su anterior perfil o su estrategia ante este incidente.

La BNP reiteró su compromiso con la transparencia y la seguridad de la información, principios que guían todas sus acciones, especialmente en un contexto de creciente digitalización de sus servicios.

3. **RECOMENDACIONES:**

- Usar contraseñas largas, complejas y únicas para cada cuenta. Considerar un gestor de contraseñas para almacenarlas de forma segura.
- Activar la autenticación de dos factores en todas tus cuentas. Usar aplicaciones como Google Authenticator es más seguro que recibir códigos por SMS.
- Mantener tus dispositivos, sistemas operativos y aplicaciones al día para protegerte de vulnerabilidades.
- Usar antivirus y antimalware para detectar amenazas.
- Ajustar las configuraciones de privacidad para limitar el acceso solo a personas de confianza. Publicar contenido solo para tu círculo cercano.
- No hacer clic en enlaces sospechosos ni descargar archivos de fuentes desconocidas. Verificar siempre la autenticidad de los correos y URLs.
- Revisar regularmente los accesos recientes a tus cuentas y configura alertas para detectar inicios de sesión sospechosos.
- Evitar usar redes Wi-Fi públicas para actividades sensibles y utilizar una VPN si es necesario.
- Realizar respaldos de tu información importante para minimizar el impacto de un posible ataque.

Fuente de Información:	• hxxps://www.infobae.com/peru/2024/11/27/biblioteca-nacional-del-peru-confirma-hackeo-de-su-cuenta-de-x-desde-donde-publicaron-material-obsceno/ • hxxps://larepublica.pe/sociedad/2024/11/27/ataque-cibernetico-a-la-biblioteca-nacional-del-peru-compromete-su-cuenta-de-x-con-contenido-inapropiado-noticias-1703187

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°274	Fecha: 27-11-2024 Página: 5 de 8

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Múltiples vulnerabilidades en productos MicroSCADA X SYS600 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 múltiples vulnerabilidades de severidad **CRÍTICA** de tipo neutralización incorrecta de elementos especiales en la lógica de consulta de datos, limitación incorrecta de una ruta a un directorio restringido ('Path Traversal'), omisión de autenticación por captura y repetición, falta de autenticación para funciones críticas y redirección de URL a un sitio no confiable ('Open Redirect') que afecta a varios de sus productos. La explotación exitosa de estas vulnerabilidades podría permitir a un atacante remoto no autenticado inyectar código en datos persistentes, manipular el sistema de archivos, secuestrar una sesión o realizar intentos de phishing contra los usuarios.

2. DETALLES:

La vulnerabilidad de severidad **crítica** identificada por MITRE como CVE-2024-4872 de tipo neutralización inadecuada de elementos especiales en la lógica de consulta de datos del producto MicroSCADA Pro/X SYS600, podría permitir que un atacante autenticado inyecte código en los datos persistentes. Se tiene que tener en cuenta que para explotar con éxito esta vulnerabilidad, un atacante debe tener una credencial válida.

La vulnerabilidad de severidad **crítica** identificada por MITRE como CVE-2024-3980 de tipo limitación incorrecta de un nombre de ruta a un directorio restringido en MicroSCADA Pro/X SYS600, podría permitir que un usuario autenticado ingrese datos para controlar o influir en las rutas o los nombres de archivos que se utilizan en las operaciones del sistema de archivos. Si se aprovecha la vulnerabilidad, el atacante puede acceder o modificar archivos del sistema u otros archivos que son críticos para la aplicación.

La vulnerabilidad de severidad **alta** identificada por MITRE como CVE-2024-3982 de tipo evitación de autenticación por capture-replay en MicroSCADA X SYS600, podría permitir a un atacante con acceso local a una máquina donde esté instalado MicroSCADA X SYS600, habilitar el registro de sesiones e intentar aprovechar un secuestro de una sesión ya establecida. De forma predeterminada, el nivel de registro de sesiones no está habilitado y solo los usuarios con derechos de administrador pueden habilitarlo.

La vulnerabilidad de severidad **alta** identificada por MITRE como CVE-2024-7940 de tipo autenticación faltante para función crítica en MicroSCADA X SYS600, podría permitir a un atacante remoto no autenticado comprometer el sistema objetivo. La vulnerabilidad existe porque el producto afectado expone un servicio destinado únicamente a uso local a todas las interfaces de red sin ninguna autenticación. Un atacante remoto puede obtener acceso al sistema de destino.

A. Productos afectados:

- Hitachi Energy MicroSCADA Pro/X SYS600: versión 10.0 a versión 10.5 (CVE-2024-4872, CVE-2024-3980, CVE-2024-3982, CVE-2024-7941).
- Hitachi Energy MicroSCADA Pro/X SYS600: versión 10.2 a versión 10.5 (CVE-2024-7940).
- Hitachi Energy MicroSCADA Pro/X SYS600: versión 9.4 FP1 (CVE-2024-3980).
- Hitachi Energy MicroSCADA Pro/X SYS600: versión 9.4 FP2 HF1 a versión 9.4 FP2 HF5 (CVE-2024-4872, CVE-2024-3980).

3. RECOMENDACIÓN:

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

Fuente de Información:	• hxxps://publisher.hitachienergy.com/preview?DocumentID=8DBD000160&LanguageCode=en&DocumentPartId=&Action=Launch • hxxps://www.cisa.gov/news-events/ics-advisories/icsa-24-331-04

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°274	Fecha: 27-11-2024 Página: 6 de 8

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad en productos North Grid Corporation		
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 **ALTA** de tipo restricción incorrecta de la referencia a una entidad externa XML que afectan a múltiples productos North Grid Corporation. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto no autenticado obtener acceso a información confidencial.

2. DETALLES:

La vulnerabilidad de severidad **alta** identificada por MITRE como CVE-2023-45727 de tipo restricción incorrecta de la referencia a una entidad externa XML en productos de North Grid Corporation, podría permitir a un atacante remoto obtener acceso a información confidencial.

La vulnerabilidad existe debido a una validación insuficiente de la entrada XML proporcionada por el usuario. Un atacante remoto puede pasar un código XML especialmente diseñado a la aplicación afectada y ver el contenido de archivos arbitrarios en el sistema o iniciar solicitudes a sistemas externos. La explotación exitosa de la vulnerabilidad puede permitir a un atacante ver el contenido de un archivo arbitrario en el servidor o realizar un escaneo de red de la infraestructura interna y externa.

A. Productos afectados:

- Proself Standard Edition: 5.62.
- Proself Enterprise Edition: 5.62.
- Proself Gateway Edition: 1.65.
- Proself Mail Sanitize Edition: 1.08.

3. RECOMENDACIÓN:

- Actualizar el producto afectado a la última versión de software disponible que aborda esta vulnerabilidad.

Fuente de Información:	• hxxps://jvn.jp/en/jp/JVN95981460/index.html • hxxps://www.proself.jp/information/153/

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°274	Fecha: 27-11-2024 Página: 7 de 8

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad de ejecución remota de código en GitHub		
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 **ALTA** de tipo inyección de comando en la Interfaz de la línea de comandos (CLI) de GitHub. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto no autenticado la ejecución de código arbitrario en la estación de trabajo del usuario, comprometiendo potencialmente los datos y el sistema del usuario.

2. DETALLES:

La vulnerabilidad de severidad **alta** identificada por MITRE como CVE-2024-52308 de tipo inyección de comando en la CLI de GitHub, podría permitir un usuario remoto comprometer el sistema afectado. La vulnerabilidad existe debido a la forma en que la CLI de GitHub maneja los detalles de la conexión SSH al ejecutar comandos. Un usuario remoto puede proporcionar un contenedor de desarrollo especialmente diseñado que pueda inyectar y ejecutar comandos arbitrarios en el sistema con privilegios elevados.

La vulnerabilidad se origina en la forma en que la CLI de GitHub maneja los detalles de la conexión SSH al ejecutar comandos. Cuando los desarrolladores se conectan a *Codespaces* remotos, normalmente usan un servidor SSH que se ejecuta dentro de un *devcontainer*, que a menudo se proporciona a través de la imagen *devcontainer* predeterminada. La CLI de GitHub recupera los detalles de la conexión SSH, como el nombre de usuario remoto, que se usa para ejecutar comandos *ssh* para "gh codespace ssh" o comandos "gh codespace logs".

Esta vulnerabilidad se produce cuando un contenedor de desarrollo de terceros malintencionado contiene un servidor SSH modificado que inyecta *ssh* argumentos dentro de los detalles de la conexión SSH *"gh codespace ssh"* y *"gh codespace logs"*. Los comandos podrían ejecutar código arbitrario en la estación de trabajo del usuario si el nombre de usuario remoto contiene algo como *-oProxyCommand="echo hacked"* #. La –o*ProxyCommand* bandera hace ssh que se ejecute el comando proporcionado mientras que el comentario de shell hace que se ignoren # los demás argumentos.

A. Productos afectados:

- Interfaz de línea de comandos de GitHub: versión 0.4.0 - 2.61.0.

3. RECOMENDACIONES:

- Actualizar el producto afectado a la versión 2.62.0 que aborda esta vulnerabilidad.
- Tener cuidado al utilizar imágenes de devcontainer personalizadas; prefiera devcontainer predeterminados o prediseñados de fuentes confiables.

Fuente de Información:	• hxxp://github.com/cli/cli/security/advisories/GHSA-p2h2-3vg9-4p87

Índice alfabético