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

132-2024-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°132	Fecha: 06-06-2024 Página: 4 de 9

Componente que reporta	CENTRO NACIONAL DE SEGURIDAD DIGITAL		
Nombre de la alerta	Honduras Enfrenta Ola de Ciberataques: Ciberdelincuentes Exigen Hasta 2 Millones por Datos Robados		
Tipo de Ataque	Ransomware	Abreviatura	Ransomware
Medios de propagación	Correo electrónico, redes sociales, entre otros		
Código de familia	C	Código de Sub familia	C01
Clasificación temática familia	Código Malicioso		

Descripción

1. ANTECEDENTES:

Honduras se encuentra bajo una creciente amenaza de ciberataques, con empresas y entidades gubernamentales sufriendo el robo de información privada, incluidos datos de usuarios. Según análisis recientes, el país centroamericano es uno de los más vulnerables a nivel global, solo superado por Bolivia.

2. DETALLES:

El estado de la ciberseguridad en Honduras es alarmante. Utilizando métricas del Índice Nacional de Seguridad Cibernética (NCSI), el Índice de Ciberseguridad Global (GCI), el Índice de Exposición a la Ciberseguridad (CEI) y estudios de Comparitech, se revela que Honduras está altamente expuesta a ciberataques. Esta situación es crítica en un contexto donde el ransomware se ha convertido en una amenaza persistente.

Scott E. Augenbaum, exagente especial del FBI, destaca que “las pequeñas y medianas empresas carecen de los recursos financieros y las habilidades para combatir la amenaza cibernética emergente”. Sin embargo, incluso las grandes empresas están siendo atacadas. El ransomware, que cifra y bloquea los accesos a los sistemas, ha afectado gravemente a maquilas, empresas financieras, de telecomunicaciones y entidades estatales.

Datos de empresas como Kaspersky y Bitdefender indican un aumento en los ataques de ransomware, con picos en enero y marzo de 2024.

Entre los grupos de ransomware más activos se encuentran LockBit 3.0, Hunter International, Blackbasta y ALPHV/BlackCat. Honduras ha sido atacada por grupos como Trigona, RansomHub y ALPHV/BlackCat, destacando la necesidad de una colaboración estrecha entre el Gobierno, empresas y expertos en ciberseguridad.

3. RECOMENDACIONES:

- Ejecutar la estrategia 3-2-1 de copias de seguridad, que consiste en realizar periódicamente tres copias de seguridad de los datos, en mínimo dos medios de almacenamiento diferentes, y albergar una de las copias fuera del sitio o en la nube.
- Cifrar las copias realizadas. Así, incluso si se ven comprometidas, serían indescifrables e inútiles para el atacante.
- Utilizar un software antimalware confiable en sus dispositivos y mantenerlos actualizados.
- Mantener su sistema operativo, software antimalware y de seguridad, y todas las aplicaciones actualizadas con los últimos parches y actualizaciones de seguridad.
- Evitar abrir archivos adjuntos o enlaces sospechosos en correos electrónicos no solicitados o mensajes de redes sociales.
- Habilitar la protección de firewall para monitorear y controlar el tráfico de red entrante y saliente.
- Educar a los usuarios sobre las amenazas de ransomware y cómo reconocer los intentos de phishing.
- No pagar el rescate ni contactar con los ciberdelincuentes, en caso de infección, ya que no hay garantía de que cumplan sus promesas. En su lugar, buscar ayuda profesional para eliminar el ransomware y restaurar los archivos cifrados. Así como también reportar el ransomware a las autoridades.

Fuente de Información:	• hxxps://devel.group/blog/honduras-enfrenta-ola-de-ciberataques-ciberdelincuentes-exigen-hasta-l2-millones-por-datos-robados/

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°132	Fecha: 06-06-2024 Página: 5 de 9

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Múltiples vulnerabilidades críticas en productos ABB		
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 reportado dos vulnerabilidades de severidad **CRÍTICA** de tipo exposición de información confidencial que afecta a varios productos de ABB que emplean los sistemas KNX que aplican el estándar KNX Data Secure. La explotación exitosa de estas vulnerabilidades permitiría a un atacante remoto conocer la clave de configuración por defecto de Fábrica (FDSK) que se utiliza durante la puesta en marcha de un producto afectado para asegurar la transmisión de la Tool-keyl, la cual asegura la conexión lógica entre un dispositivo KNX Secure y el Engineering-Tool-Software (ETS).

2. DETALLES:

La vulnerabilidad de severidad **crítica,** identificada por MITRE como CVE-2024-4008, se debe a que el dispositivo afectado no se ejecute en modo KNX Secure, mediante un mensaje específico para conocer la clave FDSK y capturar los mensajes de Telegram entre el dispositivo y el ETS. Usando la clave FDSK, se pueden descifrar las claves. Un atacante podría enviar mensajes de Telegram en nombre del dispositivo afectado.

La vulnerabilidad de severidad **crítica,** identificada por MITRE como CVE-2024-4009, se debe a que, en caso de fallo de alimentación del bus, un dispositivo vulnerable no almacena los números de secuencia de los mensajes de Telegram KNX. En consecuencia, un atacante puede capturar el último mensaje entrante y reproducirlo con un número de secuencia, incrementado que el dispositivo receptor acepta.

Las vulnerabilidades afectan exclusivamente a los sistemas KNX que aplican el estándar KNX Data Secure. Los sistemas KNX que operan en configuraciones KNX clásicas (modo simple), no están afectados.

A. Productos afectados:

- 2,4" Display 55: versión 1.00.
- 2,4" Display 63: versión 1.00.
- 2,4" Display 70: versión 1.00.
- RoomTouch 4": versión 1.00.
- Bus Compiling Unit KNX: versión 1.3.0.33.

3. RECOMENDACIONES:

- Actualizar los productos afectados a la última versión de firmware disponible que aborda estas vulnerabilidades en las respectivas versiones del producto.
- Seguir los pasos indicados a continuación, al poner en marcha una red KNX-Data-Secure:
  - Conectar el producto afectado directamente a un ordenador personal (PC) que ejecute el ETS de forma Point-to-Point (P2P). Esto garantiza que la comunicación entre ambos dispositivos no pueda ser interceptada. Los usuarios, que pueden razonablemente asumir que su Red KNX es segura, pueden incluso conectar la PC indirectamente al producto afectado a través de la red segura de datos KNX.
  - Se deben cambiar todas las claves simétricas, incluyendo la clave de la herramienta para este dispositivo, y no usar las predeterminadas.
  - Actualizar el firmware del producto afectado usando el mecanismo estándar de actualización KNX Secure.
  - Configurar el dispositivo KNX Secure según el proyecto KNX especificado en el proyecto ETS.

Fuente de Información:	• hxxps://search.abb.com/library/Download.aspx?DocumentID=9AKK108464A0803&LanguageCode=en&DocumentPartId=&Action=Launch

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°132	Fecha: 06-06-2024 Página: 6 de 9

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad de inyección de comandos en Seiko Solutions		
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 reportado una vulnerabilidad de severidad **ALTA** de tipo inyección de comandos en Seiko Solutions SkyBridge MB-A100/MB-A110 y SkyBridge BASIC MB-A130. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto ejecutar comandos arbitrarios en el sistema de destino.

2. **DETALLES:**

La vulnerabilidad de severidad **alta,** identificada por MITRE como CVE-2024-32850 de tipo inyección de comando, podrían permitir a un atacante remoto ejecutar comandos arbitrarios en el sistema de destino. La vulnerabilidad existe debido a una validación de entrada incorrecta. Un atacante remoto no autenticado puede pasar datos especialmente diseñados a la aplicación y ejecutar comandos arbitrarios en el sistema de destino. La explotación exitosa de esta vulnerabilidad puede resultar en un compromiso total del sistema vulnerable.

A. **Productos afectados:**
- SkyBridge MB-A100: 4.2.2.
- SkyBridge MB-A110: 4.2.2.
- SkyBridge BÁSICO MB-A130: 1.5.5.

3. **RECOMENDACIÓN:**

- Actualizar los productos afectados a la última versión de firmware disponible que aborda esta vulnerabilidad.

Fuente de Información:	• hxxp://www.seiko-sol.co.jp/archives/82992/ • hxxp://jvn.jp/en/vu/JVNVU94872523/

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°132	Fecha: 06-06-2024 Página: 7 de 9

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad crítica en Ovation de Emerson		
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:

Daniel dos Santos y Jos Wetzels de Forescout Technologies han reportado dos vulnerabilidades de severidad **CRÍTICA** de tipo falta de autenticación para funciones críticas y verificación insuficiente de la autenticidad de los datos en Ovation de Emerson. La explotación exitosa de estas vulnerabilidades podría permitir a un atacante remoto la ejecución remota de código, la pérdida de información confidencial, la denegación de servicio (DoS) o permitir que un atacante modifique la configuración del controlador.

2. DETALLES:

La vulnerabilidad de severidad **crítica,** identificada por MITRE como CVE-2022-29966 de tipo falta de autenticación para funciones críticas, se debe a que el producto afectado tiene varios protocolos que no tienen autenticación, lo que podría permitir a un atacante cambiar la configuración del controlador o provocar una condición de denegación de servicio.

La vulnerabilidad de severidad **alta,** identificada por MITRE como CVE-2022-30267 de tipo verificación insuficiente de la autenticidad de los datos, se debe a que el producto afectado no tiene la autenticación de firma de firmware y depende de una suma de verificación insegura para su integridad. Esto podría permitir a un atacante enviar imágenes de firmware maliciosas, provocar una condición de denegación de servicio o lograr la ejecución remota de código.

A. Productos afectados:

- Ovation: Versión 3.8.0 Feature Pack 1 y anteriores.

3. RECOMENDACIONES:

- Actualizar el producto afectado a la versión de firmware 3.8.0 Feature Pack 3 que aborda estas vulnerabilidades.
- Considerar el uso de controladores OCR3000, que ofrecen una capa adicional de protección que no está disponible para los modelos de controladores más antiguos.
- Implementar y configurar los sistemas Ovation y los componentes relacionados como se describe en el manual Ciberseguridad para sistemas Ovation (OVREF1000). Sitio web del grupo de usuarios de Ovation (Manuales de usuario - Manuales de referencia).

Fuente de Información:	• hxxps://www.cisa.gov/news-events/ics-advisories/icsa-24-158-02

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°132	Fecha: 06-06-2024 Página: 8 de 9

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad crítica en Microsoft Azure		
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 reportado una vulnerabilidad de severidad **CRÍTICA** de tipo omisión de autenticación en Microsoft Azure. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto lanzar un ataque a la cadena de suministro y ejecutar código arbitrario en los puntos finales de los clientes.

2. DETALLES:

La vulnerabilidad de severidad **crítica** de tipo omisión de autenticación en Microsoft Azure, podría permitir a un atacante remoto eludir la autenticación en Microsoft Azure. No se requiere autenticación para aprovechar esta vulnerabilidad.

La falla específica existe en los permisos otorgados a un token SAS. Un atacante puede aprovechar esta vulnerabilidad para lanzar un ataque a la cadena de suministro y ejecutar código arbitrario en los puntos finales de los clientes.

A. Productos afectados:

- Microsoft Azure.

3. RECOMENDACIÓN:

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

Fuente de Información:	• hxxps://www.zerodayinitiative.com/advisories/ZDI-24-581/ • hxxps://portal.msrc.microsoft.com/en-us/security-guidance/researcher-acknowledgments-online-services

Índice alfabético