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

ALERTA INTEGRADA DE SEGURIDAD DIGITAL

Centro Nacional de Seguridad Digital

asbanc
ASOCIACIÓN DE BANCOS DEL PERÚ

Lima, 20 de enero de 2023

017-2023-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 Aérea del 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 las empresas 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° 017	Fecha: 19-01-2023
		Página 4 de 9

Componente que reporta	**CENTRO NACIONAL DE SEGURIDAD DIGITAL**		
Nombre de la alerta	Nueva vulnerabilidad de Microsoft Azure descubierta: los expertos advierten sobre ataques RCE		
Tipo de ataque	Explotación de vulnerabilidades conocidas	Abreviatura	EVC
Medios de propagación	Red, Internet		
Código de familia	H	Código de subfamilia	H01
Clasificación temática familia	Intento de intrusión		

Descripción

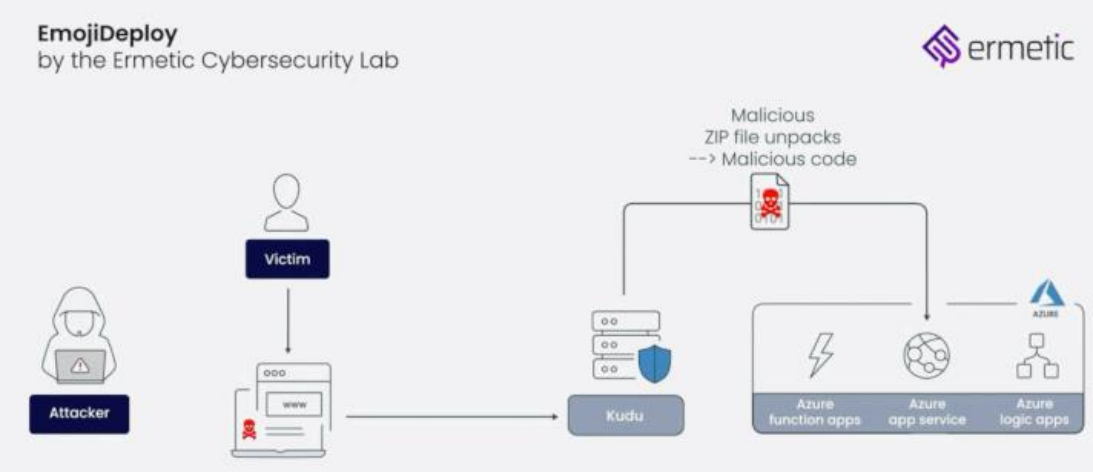
Una nueva falla crítica de ejecución remota de código (RCE) descubierta que afecta a múltiples servicios relacionados con Microsoft Azure podría ser explotada por un actor malintencionado para tomar el control completo de una aplicación específica.

DETALLES:

La vulnerabilidad se logra a través de CSRF (falsificación de solicitud entre sitios) en el ubicuo servicio SCM Kudu. Al abusar de la vulnerabilidad, los atacantes pueden implementar archivos ZIP maliciosos que contienen una carga útil en la aplicación de Azure de la víctima.

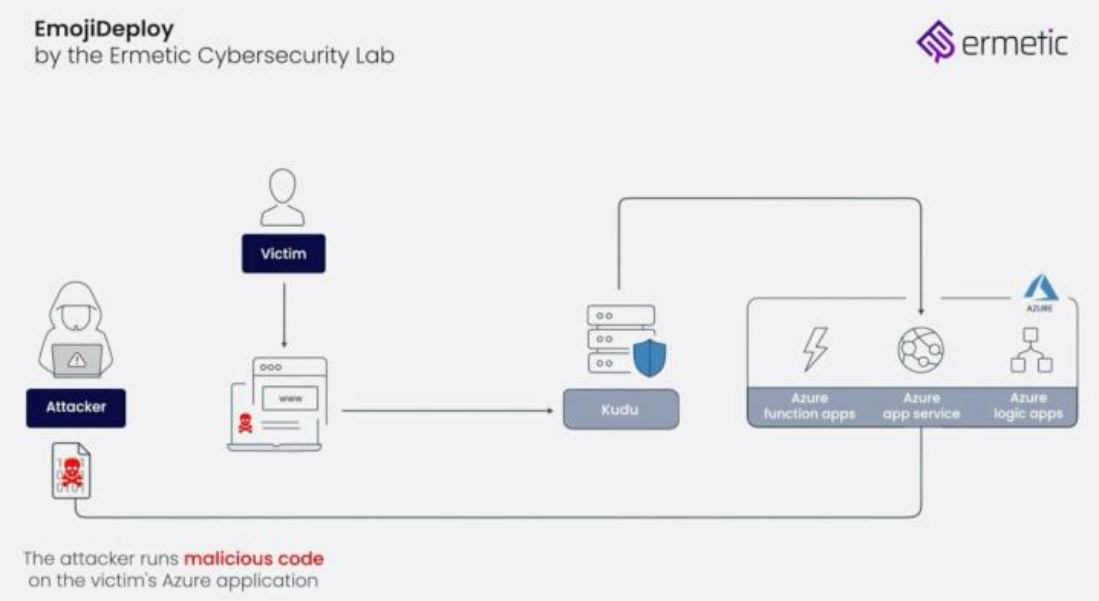
La firma israelí de seguridad de infraestructura en la nube, que denominó la deficiencia EmojiDeploy , dijo que podría permitir aún más el robo de datos confidenciales y el movimiento lateral a otros servicios de Azure. Desde entonces, Microsoft solucionó la vulnerabilidad a partir del 6 de diciembre de 2022.

El fabricante de Windows describe a Kudu como el "motor detrás de una serie de características en Azure App Service relacionadas con la implementación basada en el control de código fuente y otros métodos de implementación como Dropbox y la sincronización de OneDrive".



En una cadena de ataque hipotética ideada por Ermetic, un adversario podría explotar la vulnerabilidad CSRF en el panel Kudu SCM para vencer las medidas de seguridad implementadas para frustrar los ataques de origen cruzado mediante la emisión de una solicitud especialmente diseñada al punto final «/api/zipdeploy» para entregar un archivo malicioso (por ejemplo, web shell) y obtener acceso remoto.

La falsificación de solicitudes entre sitios, también conocida como navegación marítima o conducción de sesiones, es un vector de ataque mediante el cual un actor de amenazas engaña a un usuario autenticado de una aplicación web para que ejecute comandos no autorizados en su nombre.



El archivo ZIP, por su parte, está codificado en el cuerpo de la solicitud HTTP, lo que hace que la aplicación de la víctima navegue a un dominio de control de actores que aloja el malware a través de la omisión de la política del mismo origen del servidor.

RECOMENDACIONES:

- Microsoft recomienda que para minimizar el impacto de la vulnerabilidad depende mucho de los permisos en la aplicación, el mínimo privilegio puede limitar significativamente el radio de propagación.

Fuentes de información	▪ hxxps://thehackernews.com/2023/01/new-microsoft-azure-vulnerability.html

DINI	**ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 018**	**Fecha: 20-01-2023**
		Página 6 de 9

Componente que reporta	**DIRECCIÓN NACIONAL DE INTELIGENCIA**		
Nombre de la alerta	Múltiples vulnerabilidades en productos de Cisco		
Tipo de ataque	Explotación de vulnerabilidades conocidas	Abreviatura	EVC
Medios de propagación	Red, Internet		
Código de familia	H	Código de subfamilia	H01
Clasificación temática familia	Intento de intrusión		

Descripción

1. **Resumen:**

Cisco ha reportado dos vulnerabilidades de severidad **ALTA** y **MEDIA** de tipo inyección SQL y omisión de los filtros de reputación en varios de sus productos. La explotación exitosa de estas vulnerabilidades podría permitir a un atacante remoto autenticado realizar ataques de inyección SQL en un sistema afectado. Asimismo, un atacante remoto no autenticado podría omitir los filtros de reputación de URL en un dispositivo vulnerable.

2. **Detalles:**

- La vulnerabilidad de severidad **alta** registrada como CVE-2023-20010 en la interfaz de administración basada en web de Cisco Unified Communications Manager (Unified CM) y Cisco Unified Communications Manager Session Management Edition (Unified CM SME), podría permitir que un atacante remoto autenticado realice ataques de inyección SQL en un sistema afectado. Esta vulnerabilidad existe porque la interfaz de administración basada en web valida de manera inadecuada la entrada del usuario. Un atacante podría aprovechar esta vulnerabilidad al autenticarse en la aplicación como un usuario con pocos privilegios y enviar consultas SQL manipuladas a un sistema afectado. Una explotación exitosa podría permitir que el atacante lea o modifique cualquier dato en la base de datos subyacente o eleve sus privilegios.
- La vulnerabilidad de severidad **media** registrada como CVE-2023-20057 en el mecanismo de filtrado de URL del software Cisco AsyncOS para Cisco Email Security Appliance (ESA), podría permitir que un atacante remoto no autenticado omita los filtros de reputación de URL en un dispositivo afectado. Esta vulnerabilidad se debe a un procesamiento inadecuado de las URL. Un atacante podría explotar esta vulnerabilidad creando una URL de una manera particular. Una explotación exitosa podría permitir al atacante eludir los filtros de reputación de URL que están configurados para un dispositivo afectado, lo que podría permitir que las URL maliciosas pasen a través del dispositivo.

3. **Productos afectados:**

- La vulnerabilidad CVE-2023-20010 afecta a CM unificado y PYME de CM unificado, versión 11.5(1), 12.5(1) y 14;
- La vulnerabilidad CVE-2023-20057 afecta a todas las versiones del software Cisco AsyncOS para Cisco ESA.

4. **Solución:**

- Cisco recomienda actualizar los productos afectados con la última versión de software disponible que abordan estas vulnerabilidades.

Fuentes de información	▪ hxxps://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cucm-sql-rpPczR8n ▪ hxxps://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-esa-url-bypass-WbMQqNJh

DINI	**ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 018**	**Fecha: 20-01-2023**
		Página 7 de 9

Componente que reporta	**DIRECCIÓN NACIONAL DE INTELIGENCIA**		
Nombre de la alerta	Vulnerabilidad crítica en el núcleo de Drupal		
Tipo de ataque	Explotación de vulnerabilidades conocidas	Abreviatura	EVC
Medios de propagación	Red, Internet		
Código de familia	H	Código de subfamilia	H01
Clasificación temática familia	Intento de intrusión		

Descripción

1. **Resumen:**

   Se ha reportado una vulnerabilidad de severidad **CRÍTICA** de tipo divulgación de información que afecta a múltiples versiones del Núcleo de Drupal. La explotación exitosa de estas vulnerabilidades podría provocar que los usuarios con acceso para editar contenido vean metadatos de elementos multimedia para los que no están autorizados.

2. **Detalles:**

   - La vulnerabilidad de severidad **crítica** en el módulo de la biblioteca de medios, no verifica correctamente el acceso a la entidad en algunas circunstancias. Esto podría provocar que los usuarios con acceso para editar contenido vean metadatos de elementos multimedia para los que no están autorizados a acceder.
   - La vulnerabilidad se ve mitigada por el hecho de que los medios inaccesibles solo serán visibles para los usuarios que ya pueden editar contenido que incluye un campo de referencia de medios.

3. **Productos afectados:**

   - Versiones comprendidas entre la 8.0.0 (incluida) hasta la 9.4.10 (no incluida);
   - Versiones comprendidas entre la 9.5.0 (incluida) hasta la 9.5.2 (no incluida);
   - Versiones comprendidas entre la 10.0.0 (incluida) hasta la 10.0.2 (no incluida).

4. **Solución:**

   - El equipo de seguridad de Drupal recomienda actualizar los productos afectados con la última versión de software disponibles que abordan estas vulnerabilidades:
     - Para Drupal 10.0, actualiza a Drupal 10.0.2;
     - Para Drupal 9.5, actualiza a Drupal 9.5.2;
     - Para Drupal 9.4, actualiza a Drupal 9.4.10.
   - Cabe señalar que todas las versiones de Drupal 9 anteriores a 9.4.x están al final de su ciclo de vida y no reciben cobertura de seguridad. Asimismo, se debe de tener en cuenta que Drupal 8 ha llegado al final de su vida útil.

Fuentes de información	▪ hxxps://www.drupal.org/sa-core-2023-001

DINI	**ALERTA INTEGRADA DE SEGURIDAD DIGITAL N° 018**	**Fecha: 20-01-2023**
		Página 8 de 9

Componente que reporta	**DIRECCIÓN NACIONAL DE INTELIGENCIA**		
Nombre de la alerta	Vulnerabilidad en el PLC MELSEC iQ-F de Mitsubishi Electric Corporation		
Tipo de ataque	Explotación de vulnerabilidades conocidas	Abreviatura	EVC
Medios de propagación	Red, Internet		
Código de familia	H	Código de subfamilia	H01
Clasificación temática familia	Intento de intrusión		

Descripción

1. Resumen:

El investigador Matt Wiseman de Cisco Talos, ha reportado una vulnerabilidad de severidad **ALTA** de tipo valor exacto predecible de valores anteriores de omisión de autenticación en la funcionalidad de generación de identificadores de sesión del servidor web de MELSEC iQ-F FX5U v1.240 de Mitsubishi Electric Corporation. La explotación exitosa de esta vulnerabilidad podría provocar una fuga de cookies de sesión.

2. Detalles:

- La vulnerabilidad de severidad **alta** identificada como CVE-2022-40267 de omisión de autenticación en la funcionalidad de generación de identificadores de sesión del servidor web de MELSEC iQ-F FX5U v1.240 de Mitsubishi Electric Corporation, a través de una solicitud HTTP especialmente diseñada podría provocar una fuga de cookies de sesión. Un atacante puede enviar una serie de solicitudes HTTP para desencadenar esta vulnerabilidad.
- El iQ-F FX5U es uno de varios miembros de la serie iQ-F de controladores lógicos programables (PLC) de Mitsubishi. El FX5U viene con procesador incorporado, fuente de alimentación, ethernet y 16 puntos de E/S. El PLC se puede configurar para albergar varios servicios de red, como un servidor HTTP, un servidor FTP, un cliente FTP, una interfaz MODBUS/TCP y varios protocolos específicos de Mitsubishi.

3. Productos afectados:

- Mitsubishi Electric Corporation MELSEC iQ-F FX5U v1.240.

4. Solución:

- Se recomienda actualizar el producto afectado con la última versión de firmware disponible que aborda esta vulnerabilidad.

Fuentes de información	▪ hxxps://www.talosintelligence.com/vulnerability_reports/TALOS-2022-1646 ▪ hxxps://www.mitsubishielectric.com/fa/products/cnt/plcf/items/index.html

Índice alfabético