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

176-2024-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°176	Fecha: 31-07-2024
		Página: 4 de 8

Componente que reporta	CENTRO NACIONAL DE SEGURIDAD DIGITAL		
Nombre de la alerta	Microsoft afirma que la interrupción masiva de Azure fue causada por un ataque DDoS		
Tipo de Ataque	Denegación distribuida de servicio DDoS	Abreviatura	DDoS
Medios de propagación	Red, Correo, Navegación de Internet		
Código de familia	F	Código de Sub familia	F01
Clasificación temática familia	Disponibilidad del Servicio		

Descripción

1. **ANTECEDENTES:**

Microsoft confirmó hoy que una interrupción del servicio que duró nueve horas el martes, que paralizó e interrumpió varios servicios de Microsoft 365 y Azure en todo el mundo, fue provocada por un ataque de denegación de servicio distribuido (DDoS).

2. **DETALLES:**

Muchos usuarios informaron tener problemas para conectarse al centro de administración de Microsoft 365 y abrir la página Estado del servicio, que debería proporcionar información en tiempo real sobre los problemas que afectan a Microsoft Azure y los centros de administración de Microsoft 365/Power Platform.

Los usuarios de Reddit notaron que casi todos los servicios, incluidas las funciones de Microsoft Online, estaban inactivas o tenían un rendimiento significativamente reducido.

La compañía declaró que este incidente afectó a usuarios de todo el mundo, pero sólo a un subconjunto de sus servicios.

La interrupción afectó a Microsoft Entra, algunos servicios de Microsoft 365 y Microsoft Purview (incluidos Intune, Power BI y Power Platform), así como a Azure App Services, Application Insights, Azure IoT Central, Azure Log Search Alerts, Azure Policy y el portal de Azure.

La compañía confirmó en una declaración de mitigación publicada hoy que la causa raíz de la interrupción de ayer fue un ataque DDoS, aunque aún no lo ha vinculado a un actor de amenaza específico.

"Si bien el evento desencadenante inicial fue un ataque de denegación de servicio distribuido (DDoS), que activó nuestros mecanismos de protección DDoS, las investigaciones iniciales sugieren que un error en la implementación de nuestras defensas amplificó el impacto del ataque en lugar de mitigarlo", dijo Microsoft.

La confirmación llega después de que la compañía dijera, mientras mitigaba el incidente de interrupción, que fue causado por un "pico de uso inesperado" que "resultó en que los componentes de Azure Front Door (AFD) y Azure Content Delivery Network (CDN) tuvieran un rendimiento por debajo de los umbrales aceptables.

"La disponibilidad del servicio mejoró después de un cambio de configuración de red y algunos servicios de Microsoft 365 han realizado conmutaciones por error a rutas de red alternativas para brindar alivio. El monitoreo telemétrico muestra una mejora en la disponibilidad del servicio y continuamos monitoreando para garantizar una recuperación completa". dijo la compañía.

3. RECOMENDACIONES:

- Implementar un Firewall de aplicaciones webs para mitigar ataques de Ddos en capa 7. Implementando el WAF (Web Application Firewall) entre internet y el servidor de origen, puede servir como un proxi de reversa. Protege así el servidor objetivo de numerosos tipos de tráfico malicioso.
- Limitar el número de conexiones por dirección IP.
- Bloquear direcciones IP pertenecientes a países donde no se presta servicio.
- Activar las protecciones frente a ataques SYN Flood.
- Limitar el número de peticiones por segundo desde una misma dirección IP.
- Cerrar las conexiones HTTP lentas, no permitiendo más de unos pocos segundos entre el envío de cabeceras o contenido por parte del cliente.
- Bloquear todas las direcciones IP sospechosas de ataques DDoS utilizando Dynamic IP Restrictions (DIR).
- Bloquear peticiones con cabeceras HTTP User-Agent no estándar o pertenecientes a herramientas de hacking.
- Implementar sistemas de cache que permitan devolver peticiones sin que sean procesadas por el backend.
- Limitar el número de conexiones a los servidores de backend.
- Implementar sistemas captcha en los formularios públicos sin autenticación.
- Establecer los umbrales de las conexiones por segundo o bajar el umbral.
- Activar Mod_security y/o instalar firewall de aplicaciones destinado al servidor de aplicaciones.
- Activar Dynamic IP Restrictions (DIR).
- Regular el número de conexiones máximas simultáneas (MaxClients).
- Controlar el número de descargas desde una única dirección IP (mod_limitpconn).
- Activar mod_bwshare para permitir conexiones basadas en histórico.
- Activar mod_dosevasive módulo de apache destinado contra DDoS.
- Tener detectadas y monitorizadas las peticiones más pesadas a las bases de datos.
- Considerar las siguientes acciones, en caso de ser víctima de un Ataque DDoS
  - Eliminar las infecciones en los dispositivos comprometidos de manera individual con un software de seguridad.
  - Aislar y asegurar el tráfico usando subredes, reglas de firewall y administrar minuciosamente los accesos e identificaciones en la red.
  - Aplicar un filtrado/enrutamiento de red de tipo blackhole.
  - Desplegar instancias sin IP's públicas.
  - Habilitar el balanceador de carga basado en proxis.

Fuente de Información:	• hxxps://www.bleepingcomputer.com/news/microsoft/microsoft-says-massive-azure-outage-was-caused-by-ddos-attack/ • hxxps://www.bleepingcomputer.com/news/microsoft/microsoft-365-and-azure-outage-takes-down-multiple-services/ • hxxps://www.redhotcyber.com/post/azure-down-problemi-di-connessione-globale-per-i-servizi-microsoft/ • hxxps://telefonicatech.com/blog/ddos • hxxps://www.ikusi.com/mx/blog/como-prevenir-los-ataques-de-denegacion-de-servicio/

	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°176	Fecha: 31-07-2024
		Página: 6 de 8

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Vulnerabilidad crítica en NI VeriStand ProjectServer		
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 autorización faltante en instalaciones afectadas de NI VeriStand ProjectServer. La explotación exitosa de esta vulnerabilidad podría permitir a un atacante remoto ejecutar código arbitrario en instalaciones afectadas de NI VeriStand.

2. DETALLES:

La vulnerabilidad de severidad **crítica,** identificada por MITRE como CVE-2024-6806 de tipo autorización faltante, podría permitir a un atacante remoto ejecutar código arbitrario en instalaciones afectadas de NI VeriStand. No se requiere autenticación para explotar esta vulnerabilidad.

La falla específica existe en el procesamiento de solicitudes de servicio en el componente ProjectServer. El problema es el resultado de un método peligroso expuesto. Un atacante puede aprovechar esta vulnerabilidad para ejecutar código en el contexto del usuario actual.

A. Productos afectados:

- NI VeriStand 2024 Q2 y versiones anteriores.

3. RECOMENDACIÓN:

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

Fuente de Información:	• hxxps://www.ni.com/en/support/security/available-critical-and-security-updates-for-ni-software/missing-authorization-checks-in-ni-veristand-gateway.html • hxxps://cve.org/CVERecord?id=CVE-2024-6806

DINI	ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°176	Fecha: 31-07-2024 Página: 7 de 8

Componente que reporta	DIRECCIÓN NACIONAL DE INTELIGENCIA		
Nombre de la alerta	Múltiples vulnerabilidades en Management Center de StormShield		
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 múltiples vulnerabilidades de severidad **MEDIA** de tipo comprobación inadecuada de condiciones inusuales o excepcionales que afecta a Management Center de StormShield. La explotación exitosa de estas vulnerabilidades podría permitir a un atacante generar una condición de denegación de servicio (DoS).

2. DETALLES:

La vulnerabilidad de severidad **media,** identificada por MITRE como CVE-2023-5678 de tipo comprobación inadecuada de condiciones inusuales o excepcionales, podría permitir a un atacante que tenga acceso a la consola SMC puede usar el comando openSSL con las opciones correctas y provocar una denegación de servicio. El tiempo excesivo empleado en la verificación/generación de DH puede provocar una denegación del servicio.

La vulnerabilidad de severidad **media,** identificada por MITRE como CVE-2023-6237, podría permitir a un atacante que tenga acceso a la consola SMC usar el comando openSSL con las opciones correctas y provocar una denegación de servicio. El tiempo excesivo dedicado a verificar claves públicas RSA no válidas puede provocar una denegación de servicio.

La vulnerabilidad de severidad **media,** identificada por MITRE como CVE-2024-4603, podría permitir a un atacante que tenga acceso a la consola SMC usar el comando openSSL con las opciones correctas y provocar una denegación de servicio. La comprobación de claves o parámetros DSA excesivamente largos puede ser muy lenta.

A. Productos afectados:

- Management Center de Stormshield, versiones anteriores a 3.6.0.

3. RECOMENDACIÓN:

- Actualizar el producto afectado a la última versión de software disponible que aborda estas vulnerabilidades.

Fuente de Información:	• hxxps://advisories.stormshield.eu/2023-036/ • hxxps://advisories.stormshield.eu/2024-022/ • hxxps://advisories.stormshield.eu/2024-23/

Índice alfabético