BOLETÍN CIBERSEGURIDAD
CSIRT - DATASEC

DataSec

Storm-0501 explota Entra ID para filtrar y eliminar datos de Azure en ataques de nube híbrida

TLP:CLEAR
1.09.2025

CLICK PARA EMPEZAR

CYBERSOCDTS

En esta edición: → Storm-0501 explota Entra ID para filtrar y eliminar datos de Azure en ataques de nube híbrida

CONTENIDO

DataSec

- Nuestra Esencia
- Vulnerabilidades
- Noticias
- Recomendaciones

NUESTRA ESENCIA

BOLETÍN CIBERSEGURIDAD

Este boletín está diseñado para mantener al lector informado y brindarle pautas de seguridad en un entorno digital en constante evolución. Incluye contenido sobre las últimas amenazas, vulnerabilidades y las mejores prácticas de protección.

EMPRESA

DataSec es una empresa colombiana líder en servicios tecnológicos, enfocada en la implementación, administración, soporte, monitoreo y gestión de plataformas de Seguridad Informática y Networking, con años de experiencia en proyectos de ciberseguridad y conectividad para diversos sectores.

SOC

DataSec cuenta con un Centro de Operaciones de Seguridad Cibernética (CSOC) especializado en la detección, análisis y respuesta a amenazas. Este centro opera de manera continua 24/7, contribuyendo a la prevención y mitigación de incidentes en tiempo real.

Cisco Integrated Management Controller Virtual Keyboard Video Monitor Open Redirect Vulnerability

CVE-2025-20317

High (7.1)

Impacto: Ejecución remota de código.

Resumen: Una vulnerabilidad en el manejo de la conexión del Monitor de video de teclado virtual (vKVM) de Cisco Integrated Management Controller (IMC) podría permitir que un atacante remoto no autenticado redirija a un usuario a un sitio web malicioso.

Versiones Afectadas

- Catalyst 8300 Series Edge uCPE (CSCwo77400)
- Software UCS Manager (CSCwo04043)
- Servidores blade UCS serie B (CSCwm57436)

Solución:

Cisco ha lanzado actualizaciones de software que abordan esta vulnerabilidad.

Ver +INFO.

Fecha de Publicación: 27/AGO/2025 +INFO

Cisco Nexus 3000 and 9000 Series Switches Intermediate System-to-Intermediate System Denial of Service Vulnerability

CVE-2025-20241

High (7.4)

Impacto: Ejecución remota de código.

Resumen: Una vulnerabilidad en la función de sistema intermedio a sistema intermedio (IS-IS) del software Cisco NX-OS para switches Cisco Nexus serie 3000 y switches Cisco Nexus serie 9000 en modo NX-OS independiente podría permitir que un atacante adyacente no autenticado haga que el proceso IS-IS se reinicie inesperadamente, lo que podría hacer que un dispositivo afectado se vuelva a cargar.

Versiones Afectadas

- Nexus 3000 Series Switches
- Nexus 9000 Series Switches in standalone NX-OS mode

Solución:

Cisco ha lanzado actualizaciones de software gratuitas que abordan la vulnerabilidad descrita en este aviso.

Ver +INFO.

Fecha de Publicación: 27/AGO/2025 +INFO

IBM Engineering Lifecycle Management - Jazz Foundation is impacted by a remote attack

CVE-2025-36157

Critical (9.8)

Impacto: Denegación de servicio (DoS).

Resumen: IBM Engineering Lifecycle Management podría permitir que un atacante remoto no autenticado actualice los archivos de configuración del servidor, lo que le permitiría realizar acciones no autorizadas, lo que posteriormente conduciría a una condición de denegación de servicio.

Versiones Afectadas

- Gestión del ciclo de vida de IBM Engineering - Jazz Foundation 7.0.2
- Gestión del ciclo de vida de IBM Engineering - Jazz Foundation 7.0.3
- Gestión del ciclo de vida de IBM Engineering - Jazz Foundation 7.1.0

Solución:

- Descargue e instale 7.0.2 iFix035-sec o posterior.
- Descargue e instale 7.0.3 iFix018-sec o posterior.
- Descargue e instale 7.1.0 iFix004-sec o posterior.

Ver +INFO.

Fecha de Publicación: 22/AGO/2025 +INFO

Vulnerability in SSH authorization affects IBM

CVE-2025-36120

High (8.8)

Impacto: Escalada de privilegios.

Resumen: IBM Storage Virtualize podría permitir que un usuario autenticado escale sus privilegios en una sesión SSH debido a comprobaciones de autorización incorrectas para acceder a los recursos.

Versiones Afectadas

- IBM Storage Virtualize 8.4
- IBM Storage Virtualize 8.5
- IBM Storage Virtualize 8.6
- IBM Storage Virtualize 8.7

Solución:

Se recomienda migrar a una versión fija.

Ver +INFO.

Fecha de Publicación: 18/AGO/2025 +INFO

Actualización de seguridad para Dell Networking OS10

CVE-2024-36348, CVE-2024-36349, CVE-2024-36350, CVE-2024-36357, CVE-2024-45332

La corrección de Dell AX System for Azure Local está disponible para varias vulnerabilidades de seguridad que podrían ser explotadas por usuarios malintencionados para comprometer el sistema afectado.

Recomendación:
Actualizar a la versión foro 2503 o posterior, disponible a través del sitio web oficial del fabricante.

Versiones Afectadas

AX-760, AX-4510C, AX-4520C, AX-6515, AX-7525, AX-650 y AX-750, versiones anteriores a 2412.

Ver +INFO

Fecha de Publicación: 19/AGO/2025 INFO

Actualizaciones de seguridad de Microsoft

CVE-2025-50171, CVE-2025-50165, CVE-2025-53766, CVE-2025-24999, CVE-2025-25005

Microsoft ha lanzado las actualizaciones de seguridad correspondientes al mes de agosto, incluyendo 111 vulnerabilidades. Estas podrían permitir la denegación de servicio, la elevación de privilegios, la divulgación de información, entre otros.

Recomendación:
Actualizar a la última versión disponible a través del sitio web oficial del fabricante.

Versiones Afectadas

Azure, Desktop Windows Manager, GitHub Copilot, Visual Studio, Graphics Kernel, Kernel Streaming WOW Thunk Service Driver, Kernel Transaction Manager, Microsoft Office, Microsoft Edge, Microsoft Exchange Server Windows y otras aplicaciones de Microsoft.

Ver +INFO

Fecha de Publicación: 19/AGO/2025 INFO

LE PUEDE INTERESAR

FECHA DE PUBLICACIÓN	CVE / ACCESO	FABRICANTE	CVSSV3	DESCRIPCIÓN
20/08/2025	CVE-2025-20345	CISCO	4.9	Una vulnerabilidad en la función de registro de depuración de Cisco Duo Authentication Proxy podría permitir que un atacante remoto autenticado y con privilegios altos vea información confidencial en un archivo de registro del sistema.
20/08/2025	CVE-2025-20269	CISCO	6.5	Una vulnerabilidad en la interfaz de administración basada en web de Cisco Evolved Programmable Network Manager (EPNM) y Cisco Prime Infrastructure podría permitir que un atacante remoto autenticado y con pocos privilegios recupere archivos arbitrarios del sistema de archivos subyacente en un dispositivo afectado.
20/08/2025	CVE-2025-20131	CISCO	4.9	Una vulnerabilidad en la GUI de Cisco Identity Services Engine (ISE) podría permitir que un atacante remoto autenticado con privilegios administrativos cargue archivos en un dispositivo afectado.
27/08/2025	CVE-2025-20296	CISCO	5.4	Una vulnerabilidad en la interfaz de administración basada en web del software Cisco UCS Manager podría permitir que un atacante remoto autenticado realice un ataque de secuencias de comandos entre sitios (XSS) almacenado contra un usuario de la interfaz.
27/08/2025	CVE-2025-20294	CISCO	6.5	Múltiples vulnerabilidades en la CLI y la interfaz de administración basada en web del software Cisco UCS Manager podrían permitir que un atacante autenticado con privilegios administrativos realice ataques de inyección de comandos en un sistema afectado y eleve los privilegios a root.
27/08/2025	CVE-2025-20344	CISCO	6.5	Una vulnerabilidad en la funcionalidad de restauración de respaldo de Cisco Nexus Dashboard podría permitir que un atacante remoto autenticado realice un ataque de recorrido de ruta en un dispositivo afectado.
27/08/2025	CVE-2025-20290	CISCO	5.5	Una vulnerabilidad en la función de registro del software Cisco NX-OS para switches Cisco Nexus serie 3000, switches Cisco Nexus serie 9000 en modo NX-OS independiente, interconexiones de estructura Cisco UCS 6400, interconexiones de estructura Cisco UCS serie 6500 e interconexiones de estructura Cisco UCS 9108 100G podría permitir que un atacante local autenticado acceda a información confidencial.

Storm-0501 explota Entra ID para filtrar y eliminar datos de Azure en ataques de nube híbrida

Se ha observado que el actor de amenazas motivado financieramente conocido como Storm-0501 refina sus tácticas para realizar ataques de exfiltración y extorsión de datos dirigidos a entornos en la nube.

"A diferencia del ransomware local tradicional, donde el actor de amenazas generalmente implementa malware para cifrar archivos críticos en los puntos finales dentro de la red comprometida y luego negocia una clave de descifrado, el ransomware basado en la nube introduce un cambio fundamental", dijo el equipo de Inteligencia de Amenazas de Microsoft en un informe compartido con The Hacker News.

"Aprovechando las capacidades nativas de la nube, Storm-0501 filtra rápidamente grandes volúmenes de datos, destruye datos y copias de seguridad dentro del entorno de la víctima y exige un rescate, todo sin depender de la implementación tradicional de malware".

A continuación, compartimos IoC para ser agregados a las herramientas de seguridad perimetral.

Ver +INFO.

El ATAQUE

Storm-0501 identifica una identidad no sincronizada por humanos con un rol de administrador global en Microsoft Entra ID en ese inquilino y que carecía de protecciones de autenticación multifactor (MFA). Posteriormente, esto abrió la puerta a un escenario en el que los atacantes restablecieron la contraseña local del usuario, lo que provocó que se sincronizara con la identidad en la nube de ese usuario mediante el servicio Entra Connect Sync.

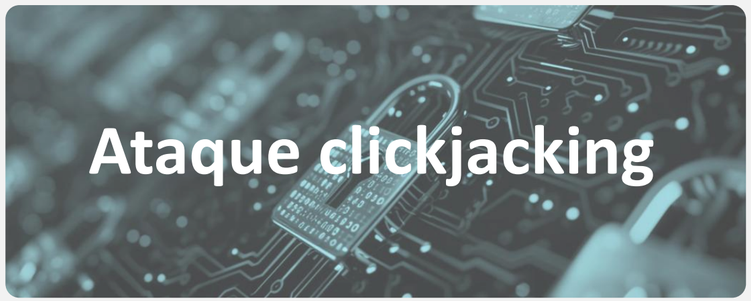
Armados con la cuenta de administrador global en peligro, se ha descubierto que los intrusos digitales acceden al Portal de Azure, registrando un inquilino de Entra ID propiedad de un actor de amenazas como un dominio federado de confianza para crear una puerta trasera y, a continuación, elevar su acceso a los recursos críticos de Azure, antes de preparar el escenario para la exfiltración y extorsión de datos.

INFO

CONTEXT	INDICATOR	(MD5)
CVE	CVE-2022-47966	N/A
CVE	CVE-2023-29300	N/A
CVE	CVE-2023-38203	N/A
CVE	CVE-2023-4966	N/A
URL	https://aadinternals[.]com/post/aad-deepdive/	N/A
URL	https://aadinternals[.]com/post/aadbackdoor/	N/A
domain	aadinternals[.]com	N/A
domain	suspectfile[.]com	N/A
PEXE - PE32 executable	caa21a8f13a0b77ff5808ad7725ff3af9b74ce5b67426c84538b8fa43820a031	92d0125f2b4187680e5fcc2c4423045b

INFO

ÚLTIMAS NOTICIAS



Ataque clickjacking

Seis de los principales gestores de contraseñas con decenas de millones de usuarios son actualmente vulnerables a fallos de clickjacking sin parches que podrían permitir a los atacantes robar credenciales de cuentas, códigos 2FA y datos de tarjetas de crédito. Podrían explotar los problemas de seguridad cuando las víctimas visitan una página maliciosa o sitios web vulnerables a secuencias de comandos entre sitios (XSS) o envenenamiento de caché

INFO

Redireccionamiento ADFS

Los piratas informáticos están utilizando una técnica novedosa que combina vínculos de office.com legítimos con Servicios de federación de Active Directory (ADFS) para redirigir a los usuarios a una página de phishing que roba inicios de sesión de Microsoft 365. El método permite a los atacantes eludir la detección tradicional basada en URL y el proceso de autenticación multifactor al aprovechar un dominio confiable en la infraestructura de Microsoft para la redirección inicial.

INFO

Fake ChatGPT

Los investigadores de ciberseguridad de Microsoft descubrieron una nueva puerta trasera llamada PipeMagic mientras investigaban ataques que abusaban de una falla de día cero en Windows CLFS (CVE-2025-29824). Lo que hace que esta puerta trasera sea peligrosa es cómo se hace pasar por una aplicación de escritorio legítima de código abierto de ChatGPT al tiempo que ofrece un marco para ejecutar operaciones de ransomware.

INFO

🔐 Tu ciberseguridad depende más de ti que de las herramientas

Aunque los sistemas de protección como firewalls, antivirus y VPNs son esenciales, la principal vulnerabilidad en ciberseguridad sigue siendo el comportamiento humano. Usar contraseñas débiles o las mismas para todo, compartir información personal sin precauciones o hacer clic en enlaces sospechosos son hábitos que abren la puerta a los cibercriminales. Las herramientas solo ayudan a mitigar los riesgos, pero si no cambiamos nuestras prácticas diarias, nuestra seguridad digital siempre estará en peligro.

🔑 Diversifica tus contraseñas: No uses la misma contraseña en varios sitios, utiliza un gestor de contraseñas para crear y almacenar contraseñas seguras y únicas para cada cuenta.
⚠️ Cuidado con los enlaces y archivos desconocidos: Antes de hacer clic, verifica la fuente y asegúrate de que el enlace o archivo sea legítimo.
🔒 Habilita la autenticación multifactor (MFA): Aunque tu contraseña sea fuerte, la MFA agrega una capa extra de protección.
🦹 No confíes ciegamente en “amigos” online: Aunque parezca un mensaje de alguien de confianza, siempre verifica antes de compartir información sensible.

DataSec | CYBERSOCDTS

csirt_datasec@datasec.com.co

+57 310 285 8969