BASELINE

INFORME EJECUTIVO MENSUAL

Boletín de Vulnerabilidades

Panorama general y criticidad en las Big Tech durante mayo. Análisis de inteligencia de seguridad sobre los hallazgos reportados, vulnerabilidades explotables y un análisis a fondo de las amenazas más críticas.

PERIODO
Mayo 2026

HALLAZGOS
6,985 CVE

ANÁLISIS GENERAL DE VULNERABILIDADES REPORTADAS POR EL NIST

Resumen ejecutivo

6,985

VULNERABILIDADES DETECTADAS EN MAYO

Un volumen sustancial de nuevos hallazgos con una composición marcadamente desplazada hacia amenazas de alto impacto que exigen atención inmediata y prioritaria.

CRÍTICAS	ALTAS	MEDIAS	BAJAS
653	2,727	2,626	616
9.3 % del total	39 % del total	38 % del total	9 % del total

Durante el mes de mayo, nuestro análisis identificó **6,985 vulnerabilidades**, con **653 clasificadas como Críticas** (≈9.3 %), **2,727 como Altas** (39 %), 2,626 como Medias (38 %) y 616 como Bajas (9 %). Esta composición refleja una tendencia alarmante hacia amenazas de alto impacto. La proporción de vulnerabilidades Críticas y Altas indica que un número considerable de estos defectos podrían ser explotados para lograr compromisos severos: ejecución remota de código, escalada de privilegios o bypass de autenticación.

Los principales fabricantes y proyectos afectados continúan siendo los pilares de la infraestructura digital: `linux_-kernel` (831), `chrome` (356), `macos` (342) y `windows` (274) encabezan la lista, lo cual es esperable dada su omnipresencia. Sin embargo, la aparición destacada de `OpenClaw` (65) y de versiones recientes como `windows_server_2025` (65), `windows_11_26h1` (60) y `windows_11_25h2` (60) sugiere una focalización creciente en software de nicho y plataformas emergentes, lo que podría indicar la evolución de los vectores de ataque.

PATRONES EN LAS VULNERABILIDADES CRÍTICAS

Vectores de ataque recurrentes

Un examen detallado de las vulnerabilidades Críticas revela patrones persistentes y peligrosos. Numerosos casos de **Ejecución Remota de Código (RCE)** fueron detectados en componentes esenciales del kernel de Linux (p. ej. `CVE-2026-31705`, `CVE-2026-31718` en ksmbd), entornos de ejecución virtual (`vm2` con múltiples escapes de sandbox) y diversas aplicaciones web y CMS (`OpenC3 COSMOS`, `Arelle`, `n8n`, `Mautic`, `ChurchCRM`, `Langflow`, `FastGPT`).

Las vulnerabilidades de **Bypass de Autenticación** y **SQL Injection** siguen siendo un vector común y eficaz, afectando a populares plugins de WordPress, plataformas de comercio electrónico (`CubeCart`, `Akilli Commerce`) y APIs de gestión (`Rucio`, `OpenC3 COSMOS`). Se identificaron además múltiples casos de **deserialización insegura** (`Apache MINA`, `Eclipse Equinox OSGi`, `Comet Backup`, `APScheduler`, `Apache Fory PyFory`) que a menudo conducen a RCE.

La presencia recurrente de **credenciales codificadas** y fallas de control de acceso en dispositivos de red e IoT (D-Link, GeoVision, Yarbo, Optoma, UniFi OS, Acer Connect) resalta una debilidad estructural en la seguridad de estos equipos. La detección de ataques a la **cadena de suministro** (paquetes `npm` como `@tanstack/*`, `DAEMON Tools Lite`) subraya la necesidad de una verificación rigurosa de todas las dependencias.

En conjunto, estos factores elevan la postura de riesgo global a un nivel crítico, exigiendo una revisión exhaustiva del inventario de activos, la priorización urgente de parches para vulnerabilidades Críticas y Altas, y la implementación de controles más robustos en la validación de entrada, la gestión de identidades y la higiene de dependencias.

INTELIGENCIA DE SEGURIDAD · MICROSOFT · GOOGLE · CISCO

Panorama Big Tech

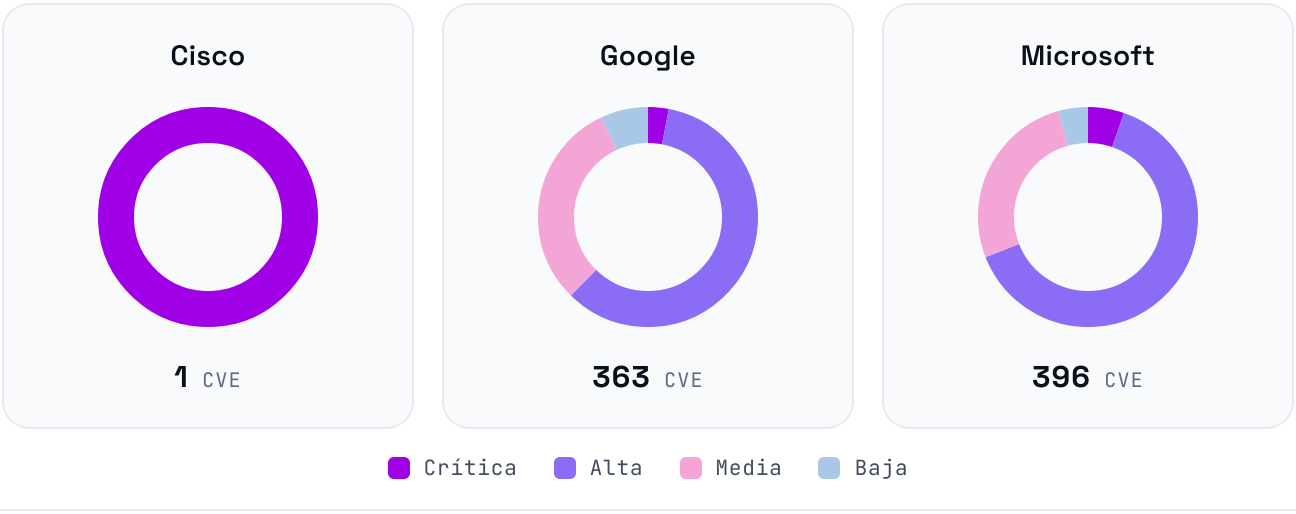
El boletín de mayo detalla el panorama de vulnerabilidades críticas y de alto riesgo identificadas en tecnologías de Big Tech, con un enfoque en Microsoft, Google y Cisco.

Microsoft registró un total de 396 vulnerabilidades, con 21 Críticas, 252 Altas, 105 Medias y 18 Bajas. La naturaleza de estas se centra predominantemente en componentes críticos de navegadores web (Blink, V8, ANGLE), indicando riesgos significativos para clientes que utilizan productos basados en Chromium. Los hallazgos clave incluyen desbordamientos de enteros y de búfer de montón, así como accesos de memoria fuera de límites, explotables remotamente para corrupción de memoria, ejecución de código en sandbox o compromiso del renderizador.

Google presentó un volumen considerable de 363 vulnerabilidades, distribuidas en 11 Críticas, 215 Altas, 111 Medias y 26 Bajas. El análisis revela una concentración en componentes de conectividad y procesamiento de comunicaciones, específicamente el subsistema IMS y sus módulos de módem, así como el daemon `adbd`. Se identificaron fallos de bypass de autenticación (`adbd_tls_verify_cert`) y múltiples vulnerabilidades de validación de entrada impropia en IMS y Modem IMS, susceptibles de causar caídas del sistema y denegación de servicio remota.

Cisco reportó un único hallazgo Crítico (`CVE-2026-20182`), sin otras vulnerabilidades clasificadas como Altas, Medias o Bajas. Aunque la información detallada es escasa, la clasificación Crítica exige una evaluación de impacto y una acción de mitigación prioritarias tan pronto como se dispongan los detalles completos.

Distribución de severidad por Big Tech



DISTRIBUCIÓN POR FABRICANTE

Severidad por marca

Conteo de vulnerabilidades por fabricante y nivel de severidad. La intensidad cromática representa el número de CVE por celda: Microsoft y Google concentran el grueso de los hallazgos de severidad Alta, mientras que Cisco presenta un único hallazgo Crítico aislado.

MICROSOFT
396
21 crít · 252 altas

GOOGLE
363
11 crít · 215 altas

CISCO
1
1 crít · 0 altas

Mapa de calor por marca y severidad

	CRÍTICA	ALTA	MEDIA	BAJA
cisco	1	0	0	0
google	11	215	111	26
microsoft	21	252	105	18

MODELO EPSS · PRÓXIMOS 30 DÍAS

Más probables a ser explotadas

Las 10 vulnerabilidades con mayor probabilidad de explotación durante los próximos 30 días, según el modelo EPSS, que estima la probabilidad de que una vulnerabilidad sea usada en un ataque real. Todas superan el 94 % de probabilidad.

CVE-2023-23752 — 94.52 %

Joomla! 4.2.8 y anteriores: divulgación de información no autenticada por falta de comprobaciones de acceso. Permite obtener configuraciones sensibles del sistema.

EPSS alto: CMS ampliamente desplegado, explotación sin autenticación y exploits públicos disponibles.

CVE-2021-22986 — 94.48 %

F5 BIG-IP y BIG-IQ: bypass de autenticación en la interfaz iControl REST. Permite ejecutar comandos del sistema con privilegios elevados, sin autenticar.

EPSS alto: dispositivos de red críticos (gateway); RCE remota no autenticada con exploits activos.

CVE-2017-8917 — 94.51 %

SAP NetWeaver AS Java 7.50 y anteriores: inyección SQL que permite ejecutar SQL arbitrario con acceso a la red, exfiltrando o modificando datos sensibles.

EPSS alto: sistema empresarial crítico; SQLi bien documentada con abundancia de herramientas y exploits.

CVE-2018-1000861 — 94.48 %

Jenkins Remoting: lectura de archivos arbitraria por el manejo de comandos. Un atacante puede leer archivos del sistema del agente.

EPSS alto: CI/CD crítico con credenciales y código fuente; escalada significativa con exploits públicos.

CVE-2018-7600 — 94.49 %

Drupal 7.x/8.x: RCE pre-autenticación («Drupalgeddon2»). Un fallo de validación permite inyectar y ejecutar código arbitrario en el servidor.

EPSS alto: RCE pre-auth en CMS masivo, control total del servidor y exploits inmediatos.

CVE-2017-1000353 — 94.48 %

Linux: falla «Stack Clash» en la gestión de la pila de memoria. Permite a un atacante local elevar privilegios a root por colisión de memoria.

EPSS alto: afecta al kernel; paso fundamental en cadenas de ataque con numerosos exploits públicos.

CVE-2018-13379

94.47 %

FortiOS: path traversal en el portal web de SSL VPN. Permite a un atacante no autenticado descargar archivos del sistema, incluidas credenciales de sesión.

EPSS alto: punto de entrada crítico a redes corporativas; pre-auth, activamente explotada por grupos APT.

CVE-2019-17558

94.47 %

Apache Solr: RCE por deserialización de código XML cuando no se requiere autenticación para JMX o no se protege el puerto de datos.

EPSS alto: componente de búsqueda empresarial popular; RCE objetivo primordial con exploits públicos.

CVE-2019-3396

94.47 %

Atlassian Confluence Server: Server-Side Template Injection vía macro Widget Connector. Permite RCE remota no autenticada en el servidor.

EPSS alto: RCE pre-auth en software de colaboración muy extendido, con exploits públicos.

CVE-2022-46169

94.47 %

Cacti: bypass de autenticación y ejecución remota de comandos vía `remote_agent.php`. Un atacante no autenticado manipula encabezados para ejecutar comandos.

EPSS alto: monitoreo de red ampliamente usado; bypass + RCE pre-auth en un solo vector, extremadamente peligroso.

! URGENCIA DE PARCHEO, CRÍTICO E INMEDIATO

Todas las CVE listadas presentan una probabilidad de explotación > 94 % según EPSS. La mayoría son vulnerabilidades pre-autenticación que conducen a RCE o comprometen la confidencialidad de sistemas críticos como VPNs, CMS, entornos CI/CD y sistemas empresariales. La amplia disponibilidad de exploits públicos y el alto impacto potencial requieren una acción correctiva prioritaria.

ANÁLISIS A FONDO · VULNERABILIDAD CRÍTICA · DIVULGACIÓN DE INFORMACIÓN

CVE-2026-42826

Microsoft Azure DevOps

CVSS 10.0

> Exposición de información sensible a un actor no autorizado en Azure DevOps que permite divulgar información a través de una red.

1 VECTOR DE ATAQUE

La vulnerabilidad se origina en una falla en la gestión o protección de la información sensible dentro de Azure DevOps. Un atacante no autorizado podría explotarla a través de la red, posiblemente mediante un endpoint de API mal configurado, una omisión de control de acceso en una interfaz web o un error lógico que expone datos sin la autenticación adecuada. La naturaleza «over a network» sugiere explotación remota sin credenciales válidas.

2 IMPACTO TÉCNICO

El impacto principal es la divulgación de información: exfiltración de código fuente propietario, secretos de despliegue, variables de entorno con credenciales, configuraciones de infraestructura o datos sensibles almacenados en repositorios, pipelines o artefactos. Esta fuga puede comprometer la propiedad intelectual y facilitar ataques de cadena de suministro.

3 JUSTIFICACIÓN DEL RIESGO

La exposición de información en un entorno DevOps es catastrófica. Azure DevOps es el corazón del ciclo de vida de desarrollo de software, y una fuga aquí puede comprometer la totalidad de los proyectos, desde la concepción hasta el despliegue, con robo de propiedad intelectual e incumplimientos normativos. El CVSS 10.0 resalta la máxima severidad de la confidencialidad comprometida.

ANÁLISIS A FONDO · VULNERABILIDAD CRÍTICA · BYPASS DE AUTENTICACIÓN

CVE-2026-20182

Cisco Catalyst SD-WAN Controller y Manager

CVSS 10.0

> Una vulnerabilidad en la autenticación de emparejamiento podría permitir a un atacante remoto no autenticado eludir la autenticación y obtener privilegios administrativos.

1 VECTOR DE ATAQUE

Es un bypass de autenticación que reside en el mecanismo de autenticación de emparejamiento y el handshaking de conexión de control de los productos SD-WAN de Cisco. Un atacante remoto y no autenticado puede explotarlo enviando peticiones manipuladas diseñadas para explotar un fallo en la lógica de autenticación durante el establecimiento de la conexión de control, eludiendo la verificación de credenciales.

2 IMPACTO TÉCNICO

Una explotación exitosa permite iniciar sesión en el Controller como una cuenta de usuario interna con altos privilegios (no root). Con este acceso, el atacante puede acceder a NETCONF, el protocolo de gestión de red, para instalar, manipular y eliminar configuraciones, obteniendo control total sobre enrutamiento, políticas de seguridad, segmentación y conectividad de la infraestructura SD-WAN.

3 JUSTIFICACIÓN DEL RIESGO

La criticidad es extrema: un atacante no autenticado con privilegios administrativos sobre la infraestructura SD-WAN puede tomar el control completo de la red. Esto habilita redirección de tráfico para exfiltración, puertas traseras persistentes y denegación de servicio total. La probabilidad de explotación activa es extremadamente alta y exige mitigación urgente.

ANÁLISIS A FONDO · VULNERABILIDAD CRÍTICA · ELEVACIÓN DE PRIVILEGIOS

CVE-2026-42822

Microsoft Azure Local Disconnected Operations

CVSS 10.0

> Autenticación incorrecta en Azure Local Disconnected Operations permite a un atacante no autorizado elevar privilegios a través de una red.

1 VECTOR DE ATAQUE

Se debe a una autenticación incorrecta en los componentes de Azure Local Disconnected Operations: el mecanismo que verifica la identidad de usuarios o procesos en un entorno que opera sin conexión principal es defectuoso. Un atacante no autorizado puede omitir completamente la autenticación o presentarse con solicitudes que el sistema acepta incorrectamente como válidas, obteniendo acceso a recursos protegidos a través de la red.

2 IMPACTO TÉCNICO

El impacto directo es la elevación de privilegios. Al eludir la autenticación, el atacante obtiene un nivel de acceso superior: control administrativo sobre el entorno local de Azure, acceso a datos sensibles almacenados localmente, o manipulación de configuraciones locales que luego podrían sincronizarse con la nube principal, afectando un espectro más amplio de la infraestructura.

3 JUSTIFICACIÓN DEL RIESGO

La elevación de privilegios es de las vulnerabilidades más peligrosas: permite pasar de ningún acceso a un control total. En entornos híbridos que dependen de Azure, el compromiso de las Local Disconnected Operations podría permitir controlar infraestructuras locales críticas, con graves implicaciones para la seguridad de datos y la continuidad operativa. El CVSS 10.0 enfatiza su criticidad máxima.

ANÁLISIS A FONDO · VULNERABILIDAD CRÍTICA · EJECUCIÓN REMOTA DE CÓDIGO

CVE-2026-23652

Microsoft Power Pages

CVSS 10.0

> Neutralización incorrecta de elementos especiales usados en un comando (command injection) en Power Pages permite ejecutar código a través de una red.

1 VECTOR DE ATAQUE

Es una inyección de comandos producida por la neutralización incorrecta de elementos especiales en la entrada procesada por Power Pages. Cuando la aplicación no sanitiza o escapa adecuadamente los caracteres con significado para el intérprete de comandos subyacente, un atacante no autorizado puede incrustar comandos maliciosos en su entrada, que el servidor ejecuta al procesarla. El ataque es remoto.

2 IMPACTO TÉCNICO

El impacto directo es la ejecución remota de código: el atacante puede ejecutar comandos arbitrarios del sistema operativo en el servidor que aloja Power Pages, obteniendo control total para desplegar malware, robar datos, modificar configuraciones, establecer persistencia o usar el servidor como pivote hacia otros sistemas internos.

3 JUSTIFICACIÓN DEL RIESGO

La RCE es de las vulnerabilidades más críticas, pues concede control total del sistema. Para organizaciones que usan Power Pages, sus aplicaciones web podrían ser comprometidas para lanzar ataques más amplios, acceder a datos de negocio o servir como punto de partida para comprometer toda la infraestructura. El CVSS 10.0 subraya la facilidad de explotación remota y sus consecuencias devastadoras.

ANÁLISIS A FONDO · VULNERABILIDAD CRÍTICA · EJECUCIÓN REMOTA DE CÓDIGO

CVE-2026-40412

Microsoft Azure Orbital Spatio

CVSS 10.0

> Carga sin restricciones de archivos con tipo peligroso en Azure Orbital Spatio permite a un atacante no autorizado ejecutar código a través de una red.

1 VECTOR DE ATAQUE

La plataforma no valida correctamente el tipo o contenido de los archivos subidos. Un atacante no autorizado puede subir un archivo malicioso, como una web shell, un script ejecutable o un archivo de configuración malformado, que el servidor considera inofensivo. Cuando ese archivo peligroso es posteriormente accedido o procesado, su código malicioso se ejecuta. La explotación se realiza de forma remota.

2 IMPACTO TÉCNICO

El impacto final es la ejecución remota de código. Al subir y activar la ejecución de un archivo malicioso, el atacante puede ejecutar código arbitrario en el servidor, obteniendo control total del sistema operativo y de los datos procesados por el servicio, lo que puede conducir a exfiltración de datos, interrupción del servicio, persistencia o movimiento lateral dentro de Azure.

3 JUSTIFICACIÓN DEL RIESGO

La RCE es una preocupación primordial. Para organizaciones que aprovechan Azure Orbital Spatio, esta falla podría permitir tomar el control de infraestructuras que procesan datos geoespaciales sensibles, resultando en robo de datos propietarios, manipulación de infraestructuras críticas o uso del entorno como base para ataques adicionales. El CVSS 10.0 destaca la máxima severidad.

ANÁLISIS A FONDO · VULNERABILIDAD CRÍTICA · DIVULGACIÓN DE INFORMACIÓN

CVE-2026-41104

Microsoft Planetary Computer Pro

CVSS 10.0

> Deserialización de datos no confiables en Planetary Computer Pro permite a un atacante no autorizado divulgar información a través de una red.

1 VECTOR DE ATAQUE

Ocurre cuando Planetary Computer Pro procesa datos serializados recibidos de un atacante no autorizado sin validación adecuada. El atacante puede incrustar objetos maliciosos o «gadgets» dentro del flujo serializado; durante la deserialización estos objetos se instancian, provocando ejecución de código inesperada o divulgación de información. El ataque es remoto y sin autenticación previa.

2 IMPACTO TÉCNICO

El impacto especificado es la divulgación de información. Aunque la deserialización suele conducir a RCE, aquí el resultado es la exposición de datos: el atacante podría diseñar datos serializados que obliguen a la aplicación a filtrar información sensible del sistema, detalles de configuración, contenido de memoria o datos como claves API, credenciales de bases de datos o detalles de la red interna.

3 JUSTIFICACIÓN DEL RIESGO

La divulgación de información de un sistema que maneja grandes volúmenes de datos ambientales y científicos puede ser extremadamente perjudicial. La fuga de algoritmos propietarios, datos de investigación o credenciales podría socavar la investigación y dar a los atacantes puntos de apoyo para una infiltración más profunda. El CVSS 10.0 indica compromiso completo de la confidencialidad desde un vector remoto y no autenticado.

ANÁLISIS A FONDO · VULNERABILIDAD CRÍTICA · ELEVACIÓN DE PRIVILEGIOS

CVE-2026-42901

Microsoft Entra ID

CVSS 10.0

> Error de validación de origen en Microsoft Entra ID permite a un atacante no autorizado elevar privilegios a través de una red.

1 VECTOR DE ATAQUE

Es un error de validación de origen en Entra ID (antes Azure AD). Se presenta cuando no se verifica correctamente el encabezado Origin en las solicitudes HTTP o no se aplica la política de mismo origen. Un atacante podría crear un sitio malicioso que engañe al navegador para realizar solicitudes a Entra ID con un origen falsificado; si no se valida, la solicitud se procesa como confiable, permitiendo manipular flujos de autenticación o sesiones.

2 IMPACTO TÉCNICO

El impacto principal es la elevación de privilegios. Al explotar el error de validación de origen, el atacante puede eludir comprobaciones de seguridad dentro de los mecanismos de autenticación de Entra ID, suplantar la identidad de otros usuarios, acceder a aplicaciones restringidas o elevar sus permisos dentro del inquilino, llegando al control administrativo sobre identidades y accesos.

3 JUSTIFICACIÓN DEL RIESGO

Entra ID es la piedra angular de la gestión de identidades para muchas organizaciones. Una elevación de privilegios aquí es profundamente crítica: el atacante podría comprometer cuentas, roles administrativos o aplicaciones empresariales, tomando el control de toda la infraestructura de identidad y habilitando filtraciones masivas, fraude financiero y control total de los recursos en la nube. El CVSS 10.0 enfatiza el impacto devastador.

ANÁLISIS A FONDO · VULNERABILIDAD CRÍTICA · ELEVACIÓN DE PRIVILEGIOS

CVE-2026-47280

Microsoft Azure Resource Manager (ARM)

CVSS 10.0

> Autenticación incorrecta en Azure Resource Manager permite a un atacante no autorizado elevar privilegios a través de una red.

1 VECTOR DE ATAQUE

ARM es el servicio de despliegue y gestión para Azure. Un atacante no autorizado puede explotar una falla en la forma en que ARM autentica las solicitudes: eludir completamente la autenticación o explotar un fallo lógico que le permita hacerse pasar por un usuario legítimo o un service principal sin credenciales adecuadas. El ataque es remoto.

2 IMPACTO TÉCNICO

El impacto directo es la elevación de privilegios. Una vez eludida la autenticación, el atacante obtiene privilegios elevados dentro de la suscripción o grupo de gestión: control sobre los despliegues de recursos, modificación de recursos existentes, eliminación de infraestructura crítica o creación de nuevos recursos bajo su control. Los privilegios en ARM otorgan control sobre toda la huella de Azure.

3 JUSTIFICACIÓN DEL RIESGO

ARM es fundamental para la gestión de todos los recursos en Azure. Una autenticación incorrecta que conduce a elevación de privilegios es de las vulnerabilidades más graves para una empresa dependiente de Azure: control administrativo completo sobre la infraestructura en la nube, filtraciones masivas, interrupciones del servicio y abuso de recursos. El CVSS 10.0 significa la máxima severidad y potencial de compromiso completo.

ANÁLISIS A FONDO · VULNERABILIDAD CRÍTICA · EJECUCIÓN REMOTA DE CÓDIGO

CVE-2026-33109

Microsoft Azure Managed Instance for Apache Cassandra

CVSS 9.9

> Control de acceso incorrecto en Azure Managed Instance for Apache Cassandra permite a un atacante autorizado ejecutar código a través de una red.

1 VECTOR DE ATAQUE

Es un control de acceso incorrecto. La clave es «atacante autorizado»: ya posee algún nivel de acceso legítimo, pero por una falla en el control de acceso puede eludir las restricciones que limitan sus acciones. Lo explota enviando solicitudes o comandos manipulados a la instancia que, en lugar de bloquearse, se procesan incorrectamente, llevando a ejecución de código no deseada. El ataque ocurre sobre la red.

2 IMPACTO TÉCNICO

El impacto es la ejecución remota de código. Pese a estar «autorizado», lograr RCE significa ejecutar código arbitrario en los servidores subyacentes que alojan la instancia de Cassandra: comprometer por completo el servidor de base de datos, acceder a todos los datos, instalar malware, pivotar a otros sistemas o interrumpir el servicio. Escala el acceso autorizado a un control total del sistema.

3 JUSTIFICACIÓN DEL RIESGO

La RCE, incluso por un usuario autorizado, es extremadamente crítica: una amenaza interna o una cuenta de bajo privilegio comprometida puede obtener control total sobre una base de datos crítica. Cassandra suele almacenar datos de negocio o altamente sensibles; la ejecución de código en el host implica exfiltración, manipulación o destrucción de datos y compromiso completo del servicio. El CVSS 9.9 destaca su muy alta severidad.

ANÁLISIS A FONDO · VULNERABILIDAD CRÍTICA · ELEVACIÓN DE PRIVILEGIOS

CVE-2026-42823

Microsoft Azure Logic Apps

CVSS 9.9

> Control de acceso incorrecto en Azure Logic Apps permite a un atacante autorizado elevar privilegios a través de una red.

1 VECTOR DE ATAQUE

Es un control de acceso incorrecto con un atacante «autorizado» que tiene acceso legítimo a alguna funcionalidad o inquilino de Logic Apps. Una falla en los mecanismos de control de acceso le permite eludir restricciones y acceder a recursos para los que carece de autorización: manipular llamadas API, configurar incorrectamente flujos de trabajo o explotar un fallo lógico en cómo se aplican los permisos entre componentes. El ataque es remoto.

2 IMPACTO TÉCNICO

El impacto es la elevación de privilegios. Al explotar la falla de control de acceso, el atacante obtiene mayores privilegios dentro de Logic Apps: control sobre otras Logic Apps, acceso a datos sensibles procesados por ellas, modificación o despliegue de nuevos flujos con permisos elevados, o acceso a servicios integrados. Elude el principio de mínimo privilegio y obtiene control más allá de su alcance asignado.

3 JUSTIFICACIÓN DEL RIESGO

Logic Apps integra procesos comerciales críticos y automatiza flujos que manejan datos sensibles y se conectan a sistemas empresariales. Una elevación de privilegios significa que un atacante con acceso inicial limitado podría comprometer la automatización crítica, interrumpir flujos, exfiltrar datos de sistemas integrados u obtener credenciales para movimiento lateral. El CVSS 9.9 subraya el riesgo severo y su amplio impacto.

SÍNTESIS Y RECOMENDACIONES

Conclusión estratégica

El mes de mayo de 2026 reveló un panorama de ciberseguridad significativamente desafiante, con casi **7,000 nuevas vulnerabilidades**. La preponderancia de hallazgos Críticos y Altos, muchos facilitando RCE o bypass de autenticación en infraestructura crítica y servicios empresariales, exige una respuesta decisiva e inmediata. La alta probabilidad de explotación activa, evidenciada por las puntuaciones EPSS, subraya una postura de riesgo elevada y la necesidad de vigilancia extrema.

Ante este escenario, es imperativo que nuestros equipos de TI empresariales adopten las siguientes recomendaciones accionables:

01 **Priorización y parcheo dirigido**

Establecer un protocolo de parcheo prioritario e inmediato para todas las vulnerabilidades Críticas (CVSS 9.9/10.0) y aquellas con EPSS superior al 80 %. Incluye plataformas de Microsoft Azure (DevOps, SD-WAN, Entra ID, Power Pages), sistemas Cisco SD-WAN y herramientas ampliamente usadas como Joomla, Drupal y Jenkins, dada su alta probabilidad de explotación activa.

02 **Refuerzo de controles fundamentales**

Fortalecer los controles de seguridad en todos los niveles: validaciones de entrada rigurosas para prevenir inyecciones de comandos y SQL, prácticas seguras de deserialización, y auditoría continua de los mecanismos de autenticación y autorización. Prestar especial atención a la higiene de la cadena de suministro, verificando la integridad de todas las dependencias.

03 **Preparación y respuesta proactiva**

Mantener una postura de seguridad proactiva mediante monitoreo continuo y caza de amenazas. Revisar y ensayar frecuentemente los planes de respuesta a incidentes, priorizando escenarios de RCE, elevación de privilegios y exfiltración de datos. La anticipación y una respuesta ágil serán claves frente a amenazas cada vez más sofisticadas y dirigidas.

BASELINE

Identifica y prioriza las vulnerabilidades de tu organización, antes que lo haga un atacante.

BOLETÍN DE VULNERABILIDADES · MAYO 2026