INGENIERÍA TELEMÁTICA S.A.S.

CIBERSEGURIDAD · REDES · CLOUD

TLP:CLEAR · INTELIGENCIA DE AMENAZAS

Edición 2026-W32 · 3 ago 2026 – 9 ago 2026

Boletín de Ciberseguridad

Resumen semanal de amenazas priorizadas, en español y con acciones claras.

RESUMEN EJECUTIVO

Esta semana, el Boletín de Ciberseguridad destaca un elevado número de vulnerabilidades críticas y de alta severidad, con seis entradas en el Catálogo KEV de CISA que requieren atención inmediata. Tres de estas son de criticidad 'Crítica' (CVSS 9.8 a 9.6), afectando a productos como IBM Langflow, JetBrains TeamCity y Progress LoadMaster, y permitiendo ejecución remota de código o inyección de comandos. También se han identificado campañas de malware sofisticadas, incluyendo el abuso de claves de Windows Hello for Business para acceso persistente a Entra ID, ataques de phishing AitM para secuestro de cuentas de Microsoft 365, y la propagación de backdoors a través de ataques a la cadena de suministro. Es fundamental que las organizaciones prioricen la aplicación de parches y refuercen sus defensas contra estas amenazas activamente explotadas.

3 Crítica 3 Alta

Publicado 10 ago 2026

Fuentes: CISA KEV, NVD y avisos de fabricante.

Ver detalle →

NIT: 816007833-0
Pereira, Colombia
+57 314 682 5259
ingenieriatelematica.com.co

VISTA RÁPIDA

Severidad CVSS · explotación activa (CISA KEV)

3	3	0	0
Crítica	Alta	Media	Baja

6 vulnerabilidades con explotación activa confirmada · 6 campaña(s) de malware · 5 noticia(s)

VULNERABILIDADES

Crítica · CVSS 9.8 EXPLOTACIÓN ACTIVA CVE-2026-9198

IBM Langflow Code Injection Vulnerability

IBM Langflow · CWE-94 — Improper Control of Generation of Code ('Code Injection') · Versiones afectadas: `1.0.0 – ≤1.10.0`

Langflow contiene una vulnerabilidad de inyección de código que permite a atacantes no autenticados lograr la ejecución remota completa de código en implementaciones predeterminadas de Langflow.

Impacto: Ejecución remota de código (RCE) completa por parte de atacantes no autenticados, lo que podría llevar al control total del sistema afectado.

> **Acción a seguir:** Actualice IBM Langflow a una versión posterior a la 1.10.0. Plazo de CISA: 2026-08-07.

Ampliar información: NVD — CVE-2026-9198 CISA KEV

Crítica · CVSS 9.8 EXPLOTACIÓN ACTIVA CVE-2026-63077

JetBrains TeamCity Deserialization of Untrusted Data Vulnerability

JetBrains TeamCity · CWE-502 — Deserialization of Untrusted Data · Versiones afectadas: `<2026.1.3, 2025.11.7`

JetBrains TeamCity presenta una vulnerabilidad de deserialización de datos no confiables que podría permitir la ejecución remota de código no autenticada a través del protocolo de sondeo del agente.

Impacto: Compromiso total del sistema afectado a través de la ejecución remota de código por atacantes no autenticados.

> **Acción a seguir:** Aplique los parches de seguridad liberados por JetBrains para TeamCity, actualizando a las versiones 2026.1.3, 2025.11.7 o posteriores. Plazo de CISA: 2026-08-08.

Ampliar información: NVD — CVE-2026-63077 CISA KEV

Crítica · CVSS 9.6 EXPLOTACIÓN ACTIVA CVE-2026-8037

Progress LoadMaster Command Injection Vulnerability

Progress LoadMaster · CWE-77 — Improper Neutralization of Special Elements used in a Command ('Command Injection') · Versiones afectadas: `V7.2.60.0 – <V7.2.63.2; V7.2.45.12 – <V7.2.54.18`

Progress LoadMaster contiene una vulnerabilidad de inyección de comandos que permite a un atacante no autenticado ejecutar comandos arbitrarios en el dispositivo LoadMaster explotando entradas no sanitizadas en múltiples puntos finales de comando.

Impacto: Ejecución arbitraria de comandos en el dispositivo LoadMaster por parte de un atacante no autenticado, lo que puede conducir al control completo del appliance.

> **Acción a seguir:** Actualice Progress LoadMaster a las versiones V7.2.63.2 o V7.2.54.18 o posteriores. Plazo de CISA: 2026-08-10.

Ampliar información: NVD — CVE-2026-8037 CISA KEV

Alta · CVSS 8.2 EXPLOTACIÓN ACTIVA CVE-2026-18556

N-able N-central Authentication Bypass Using an Alternate Path or Channel Vulnerability

N-able N-central · CWE-288 — Authentication Bypass Using an Alternate Path or Channel · Versiones afectadas: ≤2026.1

N-able N-central contiene una vulnerabilidad de omisión de autenticación que permite el acceso no autorizado a través de un camino o canal alternativo.

Impacto: Omisión de los mecanismos de autenticación, lo que puede resultar en acceso no autorizado al sistema.

> **Acción a seguir:** Actualice N-able N-central a una versión superior a la 2026.1 para mitigar la vulnerabilidad. Plazo de CISA: 2026-08-07.

Ampliar información: NVD — CVE-2026-18556 CISA KEV

Alta · CVSS 8.2 EXPLOTACIÓN ACTIVA CVE-2026-18577

N-able N-central Authentication Bypass Using an Alternate Path or Channel Vulnerability

N-able N-central · CWE-288 — Authentication Bypass Using an Alternate Path or Channel · Versiones afectadas: ≤2026.3

N-able N-central contiene una omisión de autenticación que permite el acceso no autorizado y la toma de control de cuentas. Esta vulnerabilidad es resultado de un parche incompleto para CVE-2026-18556.

Impacto: Omisión de los mecanismos de autenticación y potencial toma de control de cuentas en N-central.

> **Acción a seguir:** Actualice N-able N-central a una versión superior a la 2026.3 para mitigar la vulnerabilidad. Plazo de CISA: 2026-08-06.

Ampliar información: NVD — CVE-2026-18577 CISA KEV

Alta · CVSS 7.5 EXPLOTACIÓN ACTIVA CVE-2026-34486

Apache Tomcat Missing Encryption of Sensitive Data Vulnerability

Apache Tomcat · CWE-311 — Missing Encryption of Sensitive Data · Versiones afectadas: `11.0.20; 10.1.53; 9.0.116`

Apache Tomcat presenta una vulnerabilidad de cifrado faltante de datos sensibles que permite la omisión del EncryptInterceptor. Esta vulnerabilidad puede encadenarse con CVE-2025-24813.

Impacto: Exposición de datos sensibles debido a la omisión del cifrado, pudiendo ser explotada en conjunto con otras vulnerabilidades para mayor impacto.

> **Acción a seguir:** Actualice Apache Tomcat a las versiones 11.0.21, 10.1.54 o 9.0.117 o posteriores. Plazo de CISA: 2026-08-07.

Ampliar información: NVD — CVE-2026-34486 CISA KEV

MALWARE Y CAMPAÑAS

Malware Abusando Claves de Windows Hello for Business

Se ha identificado una técnica donde malware en entornos Windows abusa de las claves de Windows Hello for Business para obtener acceso persistente a Microsoft Entra ID. Este método permite a los atacantes mantener el control sobre las cuentas de usuario, evadiendo las defensas estándar y estableciendo persistencia en la infraestructura en la nube.

MITRE ATT&CK: `T1078.004 — Valid Accounts: Cloud Accounts`
`T1550.002 — Use Alternate Authentication: Pass the Ticket`

> **Acción a seguir:** Implemente monitoreo estricto sobre las claves de Windows Hello for Business y la actividad en Entra ID. Considere la revocación de claves comprometidas y la aplicación de políticas de acceso condicional más estrictas. Revise la configuración de seguridad de las identidades híbridas y asegure la integridad de los dispositivos para prevenir la exfiltración o el abuso de claves.

Ataques AitM Phishing: Secuestro de Cuentas Microsoft 365

Una campaña de phishing Adversary-in-the-Middle (AitM) está secuestrando cuentas de Microsoft 365 para robar credenciales y datos de nómina, evadiendo la autenticación multifactor (MFA) mediante el uso de proxies residenciales. Este tipo de ataque intercepta las sesiones de los usuarios, permitiendo a los atacantes el control de las cuentas comprometidas.

MITRE ATT&CK: `T1566.002 — Phishing: Spearphishing Link` `T1078.004 — Valid Accounts: Cloud Accounts` `T1550.002 — Use Alternate Authentication: Pass the Ticket`

> **Acción a seguir:** Concientice a los usuarios sobre las tácticas de phishing avanzado y verifique siempre la URL. Implemente MFA robusta y considere soluciones Anti-Phishing que detecten y bloqueen sitios maliciosos en tiempo real. Monitoree activamente los logs de autenticación de Microsoft 365 para detectar anomalías y accesos desde ubicaciones inusuales.

Toolkit 'khunt' y SQL Injection en Oracle para Acceso SYSTEM

Se ha descubierto cómo atacantes emplearon SQL Injection en bases de datos Oracle para compilar un toolkit personalizado llamado 'khunt' y escalar privilegios hasta obtener acceso SYSTEM en sistemas Windows, logrando evadir la detección de soluciones EDR. Esto demuestra la sofisticación de los ataques combinados para eludir las defensas perimetrales y de endpoint.

MITRE ATT&CK: `T1190 — Exploit Public-Facing Application` `T1068 — Exploitation for Privilege Escalation`

> **Acción a seguir:** Asegure sus bases de datos Oracle con las últimas actualizaciones y configuraciones de seguridad. Realice auditorías de seguridad periódicas y revise la configuración de permisos para las bases de datos. Fortalezca la segmentación de red para los servidores de bases de datos y asegure que las soluciones EDR/XDR estén configuradas para detectar comportamientos anómalos, incluso para la compilación de herramientas.

Malware Multi-etapa HollowFrame y Matryoshka

Los investigadores han detectado el cargador HollowFrame y el backdoor Matryoshka, que se despliegan mediante ataques de spear-phishing. Este malware de múltiples etapas evade las defensas tradicionales y busca persistir en entornos corporativos, permitiendo a los atacantes mantener el acceso y el control sobre los sistemas comprometidos.

MITRE ATT&CK: `T1566.001 — Phishing: Spearphishing Attachment` `T1059 — Command and Scripting Interpreter` `T1547.001 — Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder`

> **Acción a seguir:** Eduque a los empleados sobre el spear-phishing y la importancia de verificar los archivos adjuntos. Implemente soluciones de seguridad de endpoint avanzadas (EPP/EDR/XDR) con capacidades de detección de malware multi-etapa. Fortalezca la seguridad del correo electrónico con filtros robustos para adjuntos y enlaces maliciosos.

Ataque a la Cadena de Suministro de QuickFox con Backdoor FDMTP de Mustang Panda

Fortinet FortiGuard Labs ha revelado un ataque a la cadena de suministro de QuickFox, un servicio VPN, donde el instalador para Windows fue troyanizado para distribuir el backdoor FDMTP, asociado al grupo Mustang Panda. Este incidente subraya los riesgos de confiar en el software de terceros y la importancia de verificar la integridad de las descargas.

MITRE ATT&CK: `T1195.002 — Supply Chain Compromise: Compromise Software Supply Chain` `T1059 — Command and Scripting Interpreter` `T1547.001 — Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder`

> **Acción a seguir:** Verifique siempre la integridad de las descargas de software de terceros utilizando sumas de verificación o firmas digitales. Implemente controles de seguridad robustos para la cadena de suministro de software y restrinja la instalación de aplicaciones no autorizadas. Monitoree el tráfico de red para detectar comunicaciones anómalas por parte de backdoors.

PhaaS 'Greatness' evade MFA con Phishing de Código de Dispositivo

El servicio de Phishing-as-a-Service (PhaaS) 'Greatness' ha evolucionado para utilizar una técnica de phishing de código de dispositivo, permitiéndole evadir la autenticación multifactor (MFA) y robar tokens de acceso de usuarios de Microsoft 365 y Google Workspace. Este método avanzado representa una amenaza significativa para la seguridad de las cuentas en la nube.

MITRE ATT&CK: `T1566.002 — Phishing: Spearphishing Link` `T1078.004 — Valid Accounts: Cloud Accounts` `T1550.002 — Use Alternate Authentication: Pass the Ticket`

> **Acción a seguir:** Implemente MFA resistente a phishing (como FIDO2/passkeys) y eduque a los usuarios sobre las nuevas tácticas de phishing, especialmente las de código de dispositivo. Revise los logs de autenticación para detectar intentos de acceso inusuales. Refuerce las políticas de seguridad en Microsoft 365 y Google Workspace, incluyendo el monitoreo de tokens de sesión.

NOTICIAS DE CIBERSEGURIDAD

Vulnerabilidad en Google Password Manager Permite a Malware Secuestrar Cuentas con Passkeys

Se ha identificado una vulnerabilidad en Google Password Manager que, en combinación con cierto malware en Windows, permite el bypass de Passkeys de Google Chrome, facilitando accesos silenciosos y no autorizados a cuentas. Esta falla subraya la necesidad de una protección robusta en los gestores de contraseñas y un monitoreo constante del comportamiento del sistema para detectar actividades maliciosas.

Cisco Lanza Parches Urgentes para Múltiples Vulnerabilidades Críticas en SD-WAN, IOS XE e IMC

Cisco ha lanzado parches críticos para fallas con CVSS de hasta 9.9 en sus productos Catalyst SD-WAN, IOS XE e Integrated Management Controller (IMC). Algunas de estas vulnerabilidades ya cuentan con Pruebas de Concepto (PoC) disponibles, lo que incrementa el riesgo de explotación. Es crucial que las organizaciones actualicen sus sistemas Cisco de inmediato para proteger su infraestructura de red.

INC Ransomware Abusa de Vulnerabilidades Zero-Day en VPN SonicWall SMA 1000

El grupo de ransomware INC está explotando activamente las vulnerabilidades zero-day CVE-2026-15409 y CVE-2026-15410 en SonicWall SMA 1000 VPN. Estas vulnerabilidades representan un riesgo significativo para las organizaciones que utilizan estos dispositivos, ya que permiten a los atacantes acceder a la red corporativa. Se recomienda a los usuarios de SonicWall SMA 1000 revisar y aplicar las mitigaciones o parches disponibles de inmediato.

NatJack: Nuevos Ataques Secuestran Sesiones TCP y Suplantan DNS Vía Manipulación de NAT

Investigadores han descubierto NatJack, una nueva clase de ataques que manipula las tablas de Network Address Translation (NAT) para secuestrar sesiones TCP y suplantar respuestas DNS tanto en sistemas Windows como Linux. Esta técnica avanzada puede permitir a los atacantes redirigir el tráfico de red y realizar ataques 'man-in-the-middle'. Las organizaciones deben revisar sus configuraciones NAT y fortalecer la seguridad de DNS para mitigar este riesgo.

Vulnerabilidades Críticas en Veeam, Terraform y Django: CVSS 10.0 Exige Actualización Inmediata

Se han identificado y parcheado vulnerabilidades críticas, incluyendo una con CVSS 10.0, en productos ampliamente utilizados como Veeam, HashiCorp Terraform Cloud & Enterprise (MCP) y el framework Django. Estas fallas pueden permitir desde la ejecución remota de código hasta el acceso no autorizado a datos sensibles. Es imperativo que las organizaciones apliquen las actualizaciones disponibles de inmediato para proteger su infraestructura y datos críticos.

ACCIÓN A SEGUIR

Cómo te acompaña nuestro SOC

Priorice la aplicación de parches para las vulnerabilidades críticas en IBM Langflow, JetBrains TeamCity y Progress LoadMaster con fecha límite del 7 al 10 de agosto. Asegure N-able N-central y Apache Tomcat antes del 7 de agosto. Además, monitoree activamente la actividad de la red y los endpoints para detectar indicadores de compromiso relacionados con el abuso de claves de Windows Hello for Business, campañas de phishing AitM y el ransomware INC, así como la presencia de backdoors como FDMTP, HollowFrame y Matryoshka. Nuestro servicio de monitoreo y respuesta gestionada (FortiGuard SOCaaS) está disponible para reforzar sus defensas y detectar estas amenazas.

AVISO: Boletín informativo TLP:CLEAR de Ingeniería Telemática S.A.S. Datos provenientes de CISA KEV, NVD y avisos de fabricante. De carácter informativo; no sustituye un análisis de su entorno.