Boletín de alerta

Boletín Nro.:
Fecha de publicación: 19/05/2026
Tema: Alerta 2026-53 Múltiples vulnerabilidades críticas en Ivanti, Fortinet, SAP, VMware y n8n
Traffic Light Protocol (TLP): Amber

Producto(s) afectado(s):

- Ivanti Xtraction
- Productos Fortinet (FortiAuthenticator, FortiSandbox y otros componentes afectados)
- SAP NetWeaver y componentes empresariales SAP
- VMware Tools y plataformas asociadas
- n8n Automation Platform

Descripción

Diversos fabricantes han publicado actualizaciones de seguridad para múltiples vulnerabilidades críticas que afectan productos empresariales ampliamente utilizados, incluyendo soluciones de gestión, automatización, virtualización y plataformas SAP.

Entre las vulnerabilidades más relevantes se encuentran:

Ivanti Xtraction CVE-2026-8043 (CVSS 9.6)

Ivanti corrigió una vulnerabilidad crítica relacionada con el control externo de nombres de archivos, que podría permitir a un atacante autenticado leer archivos sensibles y escribir archivos HTML arbitrarios dentro del servidor web, facilitando ataques del lado cliente y exposición de información.

Fortinet CVE-2026-44277 y CVE-2026-26083 (CVSS 9.1)

Fortinet liberó parches para dos vulnerabilidades críticas:

- CVE-2026-44277: afecta FortiAuthenticator y podría permitir ejecución de código o comandos no autorizados mediante solicitudes especialmente diseñadas.
- CVE-2026-26083: afecta FortiSandbox y sus variantes cloud/PaaS, permitiendo ejecución de comandos no autorizados a través de peticiones HTTP.

SAP CVE-2026-34260 y CVE-2026-34263 (CVSS 9.6)

SAP publicó correcciones para dos fallas críticas:

- CVE-2026-34260: vulnerabilidad SQL Injection en SAP S/4HANA.
- CVE-2026-34263: ausencia de validación de autenticación en SAP Commerce Cloud.

Estas fallas podrían permitir acceso no autorizado, manipulación de información y ejecución de acciones arbitrarias dentro de entornos SAP críticos.

VMware CVE-2026-41702 (CVSS 7.8)

Broadcom ha publicado una actualización de seguridad para corregir una vulnerabilidad de alta severidad, que afecta a VMware Fusion y podría permitir a un atacante local obtener privilegios de root en sistemas comprometidos..

- CVE-2026-41702: corresponde a una condición de carrera de tipo TOCTOU (Time-of-check Time-of-use) presente durante operaciones realizadas por un binario SETUID dentro de VMware Fusion. Un atacante con privilegios locales bajos podría explotar esta falla para elevar privileios en el sistema afectado..

n8n multiples vulnerabilidades (CVSS 9.4)

Se han identificado múltiples vulnerabilidades críticas en n8n, plataforma de automatización de flujos de trabajo, que podrían permitir a un atacante autenticado ejecutar código remoto, leer archivos arbitrarios del servidor o comprometer la instancia afectada..

- CVE-2026-42231: contaminación de prototipos mediante el procesamiento de cuerpos XML en webhooks usando xml2js, con posible RCE al encadenarse con operaciones SSH del nodo Git.
- CVE-2026-42232: contaminación global de prototipos mediante el XML Node, lo que puede derivar en RCE al combinarse con otros nodos.
- CVE-2026-44791: bypass del parche previo asociado a CVE-2026-42232 en el XML Node, con posible RCE.
- CVE-2026-44789: contaminación de prototipos mediante un parámetro de paginación no validado en el nodo HTTP Request, con posible RCE.
- CVE-2026-44790: inyección de flags CLI en la operación Push del nodo Git, permitiendo lectura arbitraria de archivos del servidor y posible compromiso total.

Solución:

Se recomiendan la siguientes acciones de forma inmediata:

- Actualizar a Ivanti Xtraction 2026.2
- Actualizar a FortiAuthenticator 6.5.7 o 6.6.9 o 8.0.3

- Actualizar a FortiSandbox 4.4.9 o 5.0.2
- Actualizar a la nota de seguridad publicada por SAP como “May 2026 Patch Day”
- Actualizar VMware Fusion a la versión corregida 26H1
- Actualizar n8n a versiones 1.123.43, 2.20.7 o 2.22.1, o superiores.

Información adicional:

- https://thehackernews.com/2026/05/ivanti-fortinet-sap-vmware-n8n-patch.html
- https://ccb.belgium.be/advisories/warning-critical-vulnerabilities-n8n-patch-immediately-0
- https://www.scworld.com/brief/broadcom-patches-high-severity-vmware-fusion-flaw-allowing-local-privilege-escalation
- https://www.securityweek.com/fortinet-ivanti-patch-critical-vulnerabilities/
- https://techmaniacs.com/2026/05/18/cybersecurity-daily-briefing-may-18-2026/