El día de ayer fue martes de parches (Patch Tuesday), lo que significa que diversos proveedores de software han publicado actualizaciones para corregir múltiples vulnerabilidades de seguridad que afectan a sus productos y servicios.

Microsoft lanzó correcciones para 59 fallos, entre ellos seis vulnerabilidades de día cero que están siendo explotadas activamente en distintos componentes de Windows. Estas fallas podrían aprovecharse para eludir mecanismos de seguridad, escalar privilegios y provocar condiciones de denegación de servicio (DoS).

Por su parte, Adobe publicó actualizaciones para Audition, After Effects, InDesign Desktop, Substance 3D, Bridge, Lightroom Classic y el SDK de DNG. La compañía indicó que no tiene conocimiento de que estas vulnerabilidades estén siendo explotadas activamente.

SAP distribuyó parches para dos vulnerabilidades críticas, incluida una falla de inyección de código en SAP CRM y SAP S/4HANA (CVE-2026-0488, puntuación CVSS: 9.9), que podría permitir a un atacante autenticado ejecutar sentencias SQL arbitrarias y comprometer completamente la base de datos.

La segunda vulnerabilidad crítica corresponde a la ausencia de una verificación de autorización en SAP NetWeaver Application Server ABAP y ABAP Platform (CVE-2026-0509, puntuación CVSS: 9.6), lo que podría permitir que un usuario autenticado con bajos privilegios ejecute determinadas llamadas remotas a funciones en segundo plano sin contar con la autorización S_RFC requerida.

*«Para corregir la vulnerabilidad, los clientes deben implementar una actualización del kernel y configurar un parámetro de perfil»*, señaló Onapsis. *«También podrían ser necesarios ajustes en los roles de usuario y en la configuración de UCON para evitar interrupciones en los procesos de negocio.»*

Para completar la lista, Intel y Google informaron que colaboraron en la evaluación de seguridad de Intel Trust Domain Extensions (TDX) 1.5, identificando cinco vulnerabilidades en el módulo (CVE-2025-32007, CVE-2025-27940, CVE-2025-30513, CVE-2025-27572 y

CVE-2025-32467), además de cerca de tres decenas de debilidades, errores y recomendaciones de mejora.

*«Intel TDX 1.5 incorpora nuevas funciones y capacidades que acercan significativamente la computación confidencial a la paridad funcional con las soluciones tradicionales de virtualización»*, indicó Google. *«Sin embargo, estas mejoras también han incrementado la complejidad de un componente de software con altos privilegios dentro de la TCB [Trusted Computing Base].»*

## Parches de software de otros proveedores

En las últimas semanas, otros fabricantes también han publicado actualizaciones de seguridad para corregir diversas vulnerabilidades, entre ellos —

ABB
Amazon Web Services
AMD
AMI
Apple
ASUS
AutomationDirect
AVEVA
Broadcom (incluido VMware)
Canon
Check Point
Cisco
Citrix
Commvault
ConnectWise
D-Link
Dassault Systèmes
Dell

Devolutions
dormakaba
Drupal
F5
Fortinet
Foxit Software
FUJIFILM
Fujitsu
Gigabyte
GitLab
Google Android y Pixel
Google Chrome
Google Cloud
Grafana
Hikvision
Hitachi Energy
HP
HP Enterprise (incluyendo Aruba Networking y Juniper Networks)
IBM
Intel
Ivanti
Lenovo
Distribuciones Linux como AlmaLinux, Alpine Linux, Amazon Linux, Arch Linux, Debian, Gentoo, Oracle Linux, Mageia, Red Hat, Rocky Linux, SUSE y Ubuntu
MediaTek
Mitsubishi Electric
MongoDB
Moxa
Mozilla Firefox y Thunderbird
n8n
NVIDIA
Phoenix Contact

QNAP
Qualcomm
Ricoh
Rockwell Automation
Samsung
Schneider Electric
ServiceNow
Siemens
SolarWinds
Splunk
Spring Framework
Supermicro
Synology
TP-Link
WatchGuard
Zoho ManageEngine
Zoom, y
Zyxel