Daily brief, Saturday, August 22, 2026

Aug 21, 8:00 PM to Aug 22, 8:00 PM ET

Generated Nov 2, 2026, 5:37 AM ET

0	0	0	36	0	1
Breaking	Newly exploited	Exploit code	Critical CVEs	Ransomware posts	New breaches

36 new critical CVEs, 1 new breaches.

Breaking

Nothing spreading fast in technology large companies run.

Newly exploited in the wild

No CVEs added to CISA's known-exploited list.

New public exploit code

No new Nuclei templates, Metasploit modules, Exploit-DB or VulnCheck XDB entries.

New critical CVEs

36

10.0 **CVE-2026-77946**

A vulnerability was determined in TRENDnet TEW-821DAP 2.2.01b05. Affected by this vulnerability is the function uci_safe_get of the file /cgi-bin/apply_time.cgi of the component NTP Timezone Configuration Handler. Executing a manipulation of the argument syste

10.0 **CVE-2026-76604**

Joomla Extension - fabrikar.com - Unauthenticated remote code execution via PHP form element in Fabrik < 4.7.2 - The PHP form element is vulnerable to the execution of user provided codes.

10.0 **CVE-2026-76605**

Joomla Extension - fabrikar.com - Remote code execution via image element in Fabrik < 4.7.2.

10.0 **CVE-2026-76606**

Joomla Extension - fabrikar.com - Path Traversal via image element in Fabrik < 4.7.2.

10.0 **CVE-2026-76607**

Joomla Extension - fabrikar.com - Missing ACL check in download element in Fabrik < 4.7.2.

10.0 **CVE-2026-74612**

In the Linux kernel, the following vulnerability has been resolved: veth: fix skb length accounting after XDP frag adjustment veth exposes non-linear skb fragments through an xdp_buff. If an XDP program adjusts the fragment area, veth_xdp_rcv_skb() copies xdp_

10.0 **CVE-2026-74705**

In the Linux kernel, the following vulnerability has been resolved: udp: fix potential use-after-free in tunnel segmentation __skb_udp_tunnel_segment() gets the UDP header before ensuring the tunnel header is in the skb head. If the pull reallocates skb->head,

9.8 **CVE-2026-77000**

The WP Social Media Login WordPress plugin through 1.0.6 does not verify that a social login was actually completed with the identity provider before authenticating a visitor, allowing unauthenticated attackers to log in as any existing user, including adminis

9.8 **CVE-2026-77001**

The Social Login & Sharing buttons with Analytics By SoClever WordPress plugin through 1.2.0 does not perform any authentication, authorisation or nonce checks in one of its publicly accessible login handlers, allowing unauthenticated attackers to obtain a val

9.8 **CVE-2026-77002**

The SmilePass Selfie Login WordPress plugin through 1.0.2 does not perform any server-side verification of the identity it is asked to authenticate, allowing unauthenticated users to log in as any registered account, including administrators.

9.8 **CVE-2026-78003**

The Mailgun for WordPress plugin for WordPress is vulnerable to Server-Side Request Forgery (SSRF) via path traversal in versions up to and including 2.2.0. This is due to insufficient input validation in the add_list() function, which accepts user-controlled

9.8 **CVE-2026-4703**

The WS Form LITE – Drag & Drop Contact Form Builder plugin for WordPress is vulnerable to PHP Object Injection in all versions up to, and including, 1.10.80 via deserialization of untrusted input from form submission meta values. This makes it possible for una

9.8 **CVE-2026-74586**

In the Linux kernel, the following vulnerability has been resolved: sctp: clear new_transport when removing a peer sctp_process_asconf_param() stores a newly added peer transport in asoc->new_transport. After all parameters in the ASCONF chunk have been proces

9.8 **CVE-2026-74587**

In the Linux kernel, the following vulnerability has been resolved: sctp: fix use-after-free of cached ASCONF chunk addip_last_asconf caches the outstanding outbound ASCONF chunk. The normal ASCONF-ACK completion path releases the chunk and clears the pointer.

9.8 **CVE-2026-74588**

In the Linux kernel, the following vulnerability has been resolved: sctp: keep chunk->transport in step with the list it is queued on __sctp_outq_flush_rtx() moves a gap-acked chunk onto another transport's transmitted list without updating chunk->transport: i

9.8 **CVE-2026-74591**

In the Linux kernel, the following vulnerability has been resolved: mm/filemap: __filemap_add_folio() restore index before retrying In __filemap_add_folio()'s split-a-conflict loop, xas_set_order() is applied repeatedly: each application modifies xas.xa_index,

9.8 **CVE-2026-74597**

In the Linux kernel, the following vulnerability has been resolved: ip6_tunnel: clear skb2->cb[] in ip6ip6_err() ip6ip6_err() clones an outer IPv6 ICMP error skb, pulls it to the quoted inner IPv6 packet, and then passes the clone to icmpv6_send(). The clone s

9.8 **CVE-2026-74608**

In the Linux kernel, the following vulnerability has been resolved: smb: client: Fix use-after-free in cifs_try_adding_channels() cifs_try_adding_channels() takes a temporary reference to an interface before dropping iface_lock. If cifs_ses_add_channel() fails

9.8 **CVE-2026-74611**

In the Linux kernel, the following vulnerability has been resolved: tls: rx: restore msg_iter before TLS 1.3 optimistic retry tls_decrypt_sg() advances msg->msg_iter when it maps user pages for the optimistic TLS 1.3 zero-copy path. If the decrypted record tur

9.8 **CVE-2026-74616**

In the Linux kernel, the following vulnerability has been resolved: xdp: reject clones that overrun skb_shared_info tailroom xdpf_clone() clones broadcast copies into a single page and sets frame_sz to PAGE_SIZE. __xdp_build_skb_from_frame() later treats that

16 more critical CVEs in this window: see the dashboard

Ransomware

No leak-site posts collected.

New data breaches 1

Golf Canada golfcanada.ca 568,972 accounts

Watch Floor collects CVE records, CISA KEV, exploit indexes, official advisories, security news and chatter. CVSS is the headline score. Ransomware posts are criminal groups' claims, not confirmed by the victims. CVE IDs link to the full record on Watch Floor.