Daily brief, Saturday, March 28, 2026

Mar 27, 8:00 PM to Mar 28, 8:00 PM ET

Generated Nov 7, 2026, 10:29 AM ET

0	0	0	10	0	0
Breaking	Newly exploited	Exploit code	Critical CVEs	Ransomware posts	New breaches

10 new critical CVEs.

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

10

9.8 **CVE-2016-20049** Varaneckas jad java decompiler

JAD 1.5.8e-1kali1 and prior contains a stack-based buffer overflow vulnerability that allows attackers to execute arbitrary code by supplying oversized input that exceeds buffer boundaries. Attackers can craft malicious input strings exceeding 8150 bytes to ov

9.8 **CVE-2017-20227** Varaneckas jad java decompiler

JAD Java Decompiler 1.5.8e-1kali1 and prior contains a stack-based buffer overflow vulnerability that allows attackers to execute arbitrary code by supplying overly long input that exceeds buffer boundaries. Attackers can craft malicious input passed to the ja

9.8 **CVE-2018-25223** Ftnapps crashmail ii

Crashmail 1.6 contains a stack-based buffer overflow vulnerability that allows remote attackers to execute arbitrary code by sending malicious input to the application. Attackers can craft payloads with ROP chains to achieve code execution in the application c

9.8 **CVE-2018-25221** Echatserver easy chat server

EChat Server 3.1 contains a buffer overflow vulnerability in the chat.ghp endpoint that allows remote attackers to execute arbitrary code by supplying an oversized username parameter. Attackers can send a GET request to chat.ghp with a malicious username value

9.8 **CVE-2017-20225** Ticalc tiemu

TiEmu 2.08 and prior contains a stack-based buffer overflow vulnerability that allows attackers to execute arbitrary code by exploiting inadequate boundary checks on user-supplied input. Attackers can trigger the overflow through command-line arguments passed

9.8 **CVE-2018-25220** Bochs Project bochs

Bochs 2.6-5 contains a stack-based buffer overflow vulnerability that allows attackers to execute arbitrary code by supplying an oversized input string to the application. Attackers can craft a malicious payload with 1200 bytes of padding followed by a return-

9.8 **CVE-2017-20229** Invisible-Island mawk

MAWK 1.3.3-17 and prior contains a stack-based buffer overflow vulnerability that allows attackers to execute arbitrary code by exploiting inadequate boundary checks on user-supplied input. Attackers can craft malicious input that overflows the stack buffer an

9.8 **CVE-2026-3256** Ktat http\

HTTP::Session versions before 0.54 for Perl defaults to using insecurely generated session ids. HTTP::Session defaults to using HTTP::Session::ID::SHA1 to generate session ids using a SHA-1 hash seeded with the built-in rand function, the high resolution epoch

9.8 **CVE-2025-15604** Tokuhirom amon2

Amon2 versions before 6.17 for Perl use an insecure random_string implementation for security functions. In versions 6.06 through 6.16, the random_string function will attempt to read bytes from the /dev/urandom device, but if that is unavailable then it gener

9.8 **CVE-2025-9497** Microchip timeprovider 4100 firmware

Use of Hard-coded Credentials vulnerability in Microchip Time Provider 4100 allows Malicious Manual Software Update.This issue affects Time Provider 4100: before 2.5.0.

Ransomware

No leak-site posts collected.

New data breaches

No new breaches published.

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. Leak-site data: RansomLook (ransomlook.io), CC BY 4.0; sectors grouped and countries mapped by Watch Floor. CVE IDs link to the full record on Watch Floor.