Daily brief, Tuesday, April 28, 2026

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

Generated Nov 7, 2026, 4:48 AM ET

0	2	0	19	0	0
Breaking	Newly exploited	Exploit code	Critical CVEs	Ransomware posts	New breaches

2 newly exploited, 19 new critical CVEs.

Breaking

Nothing spreading fast in technology large companies run.

Newly exploited in the wild 2

8.4 **CVE-2024-1708** ConnectWise ScreenConnect CISA KEV DETECTION

Path traversal in ConnectWise ScreenConnect lets an attacker execute remote code or access confidential data and critical systems.

4.3 **CVE-2026-32202** Microsoft Windows CISA KEV

An unauthorized remote attacker can perform spoofing over a network against Microsoft Windows Shell due to a protection mechanism failure (CWE-693).

New public exploit code

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

New critical CVEs 19

9.6 **CVE-2026-7321** Mozilla firefox

Sandbox escape due to incorrect boundary conditions in the WebRTC: Networking component. This vulnerability was fixed in Firefox 150, Thunderbird 150, Firefox ESR 140.10.1, and Thunderbird 140.10.1.

9.6 **CVE-2026-7333** Google chrome

Use after free in GPU in Google Chrome prior to 147.0.7727.138 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)

9.1 **CVE-2026-40976** Vmware spring boot

In certain circumstances, Spring Boot's default web security is ineffective allowing unauthorized access to all endpoints. For an application to be vulnerable, it must: be a servlet-based web application; have no Spring Security configuration of its own and re

9.8 **CVE-2026-24178** Nvidia nvflare

NVIDIA NVFlare Dashboard contains a vulnerability in the user management and authentication system where an unauthenticated attacker may cause authorization bypass through user-controlled key. A successful exploit of this vulnerability may lead to privilege es

9.8 **CVE-2026-41873** Apache pony mail

** UNSUPPORTED WHEN ASSIGNED ** Inconsistent Interpretation of HTTP Requests ('HTTP Request/Response Smuggling') vulnerability in Pony Mail leading to admin account takeover. This issue affects all versions of the Lua implementation of Pony Mail. There is a Py

9.4 **CVE-2026-3893** Carlson Software VASCO-B GNSS Receiver

The Carlson VASCO-B GNSS Receiver lacks an authentication mechanism, allowing an attacker with network access to directly access and modify its configuration and operational functions without needing credentials.

9.8 **CVE-2026-32644**

Specific firmware versions of Milesight AIOT cameras use SSL certificates with default private keys.

9.8 **CVE-2026-7202**

A vulnerability has been found in Totolink A8000RU 7.1cu.643_b20200521. This affects the function setWiFiWpsStart of the file /cgi-bin/cstecgi.cgi of the component CGI Handler. The manipulation of the argument wscDisabled leads to os command injection. The att

9.8 **CVE-2026-7203**

A vulnerability was found in Totolink A8000RU 7.1cu.643_b20200521. This vulnerability affects the function setUrlFilterRules of the file /cgi-bin/cstecgi.cgi of the component CGI Handler. The manipulation of the argument enable results in os command injection.

9.8 **CVE-2026-7204**

A vulnerability was determined in Totolink A8000RU 7.1cu.643_b20200521. This issue affects the function setPptpServerCfg of the file /cgi-bin/cstecgi.cgi of the component CGI Handler. This manipulation of the argument enable causes os command injection. The at

9.8 **CVE-2026-7240**

A vulnerability has been found in Totolink A8000RU 7.1cu.643_b20200521. This vulnerability affects the function setVpnAccountCfg of the file /cgi-bin/cstecgi.cgi of the component CGI Handler. Such manipulation of the argument User leads to os command injection

9.8 **CVE-2026-7241**

A vulnerability was found in Totolink A8000RU 7.1cu.643_b20200521. This issue affects the function setWiFiBasicCfg of the file /cgi-bin/cstecgi.cgi of the component CGI Handler. Performing a manipulation of the argument wifiOff results in os command injection.

9.8 **CVE-2026-7242**

A vulnerability was determined in Totolink A8000RU 7.1cu.643_b20200521. Impacted is the function setOpenVpnClientCfg of the file /cgi-bin/cstecgi.cgi of the component CGI Handler. Executing a manipulation of the argument enabled can lead to os command injectio

9.8 **CVE-2026-7243**

A vulnerability was identified in Totolink A8000RU 7.1cu.643_b20200521. The affected element is the function setRadvdCfg of the file /cgi-bin/cstecgi.cgi of the component CGI Handler. The manipulation of the argument maxRtrAdvInterval leads to os command injec

9.8 **CVE-2026-7244**

A security flaw has been discovered in Totolink A8000RU 7.1cu.643_b20200521. The impacted element is the function setWiFiEasyGuestCfg of the file /cgi-bin/cstecgi.cgi of the component CGI Handler. The manipulation of the argument merge results in os command in

9.8 **CVE-2026-7248** Dlink di-8100 firmware

A vulnerability was found in D-Link DI-8100 16.07.26A1. This affects the function tgfile_htm of the file tgfile.htm of the component CGI Endpoint. The manipulation of the argument fn results in buffer overflow. The attack can be executed remotely. The exploit

9.8 **CVE-2025-60889** Stellar-Group hpx

Insecure deserialization of untrusted input in StellarGroup HPX 1.11.0 under certain conditions may allow attackers to execute arbitrary code or other unspecified impacts.

9.8 **CVE-2026-41446**

Snap One WattBox 800 and 820 series firmware versions prior to 2.10.0.0 contain undisclosed diagnostic HTTP endpoints that require only the device MAC address and service tag for authentication, both of which are printed in plaintext on the physical device lab

9.1 **CVE-2026-41386** Openclaw openclaw

OpenClaw before 2026.3.22 contains a privilege escalation vulnerability where bootstrap setup codes are not bound to intended device roles and scopes during pairing. Attackers can exploit this during first-use device pairing to escalate privileges beyond their

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.