Daily brief, Monday, March 16, 2026

Mar 15, 8:00 PM to Mar 16, 8:00 PM ET

Generated Nov 7, 2026, 12:56 PM ET

0	1	0	31	0	0
Breaking	Newly exploited	Exploit code	Critical CVEs	Ransomware posts	New breaches

1 newly exploited, 31 new critical CVEs.

Breaking

Nothing spreading fast in technology large companies run.

Newly exploited in the wild

1

4.3 **CVE-2025-47813** Wing FTP Server Wing FTP Server CISA KEV DETECTION

Wing FTP Server leaks sensitive information through error messages when a long value is supplied in the UID cookie, exposing data to an attacker.

New public exploit code

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

New critical CVEs

31

9.8 **CVE-2026-32267** Craftcms craft cms

Craft CMS is a content management system (CMS). From version 4.0.0-RC1 to before version 4.17.6 and from version 5.0.0-RC1 to before version 5.9.12, a low-privilege user (or an unauthenticated user who has been sent a shared URL) can escalate their privileges

9.8 **CVE-2026-4170**

A weakness has been identified in Topsec TopACM 3.0. Affected by this vulnerability is an unknown functionality of the file /view/systemConfig/management/nmc_sync.php of the component HTTP Request Handler. Executing a manipulation of the argument template_path

9.8 **CVE-2026-4163**

A vulnerability was detected in Wavlink WL-WN579A3 220323. This issue affects the function SetName/GuestWifi of the file /cgi-bin/wireless.cgi of the component POST Request Handler. Performing a manipulation results in command injection. It is possible to init

9.8 **CVE-2025-69902**

A command injection vulnerability in the minimal_wrapper.py component of kubectl-mcp-server v1.2.0 allows attackers to execute arbitrary commands via injecting arbitrary shell metacharacters.

9.8 **CVE-2026-4164**

A flaw has been found in Wavlink WL-WN578W2 221110. Impacted is the function Delete_Mac_list/SetName/GuestWifi of the file /cgi-bin/wireless.cgi of the component POST Request Handler. Executing a manipulation can lead to command injection. It is possible to la

9.8 **CVE-2025-15060**

claude-hovercraft executeClaudeCode Command Injection Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of claude-hovercraft. Authentication is not required to exploit this vulne

9.8 **CVE-2026-4252** Tenda ac8 firmware

A vulnerability was identified in Tenda AC8 16.03.50.11. Affected by this issue is the function check_is_ipv6 of the component IPv6 Handler. The manipulation leads to reliance on ip address for authentication. It is possible to initiate the attack remotely. Th

9.8 **CVE-2026-4181** Dlink dir-816 firmware

A security flaw has been discovered in D-Link DIR-816 1.10CNB05. This affects an unknown function of the file /goform/form2RepeaterStep2.cgi of the component goahead. The manipulation of the argument key1/key2/key3/key4/pskValue results in stack-based buffer o

9.8 **CVE-2026-4183** Dlink dir-816 firmware

A security vulnerability has been detected in D-Link DIR-816 1.10CNB05. Affected is an unknown function of the file /goform/form2WlanBasicSetup.cgi of the component goahead. Such manipulation of the argument pskValue leads to stack-based buffer overflow. The a

9.8 **CVE-2026-4184** Dlink dir-816 firmware

A vulnerability was detected in D-Link DIR-816 1.10CNB05. Affected by this vulnerability is an unknown functionality of the file /goform/form2Wl5BasicSetup.cgi of the component goahead. Performing a manipulation of the argument pskValue results in stack-based

9.8 **CVE-2026-4182** Dlink dir-816 firmware

A weakness has been identified in D-Link DIR-816 1.10CNB05. This impacts an unknown function of the file /goform/form2Wl5RepeaterStep2.cgi of the component goahead. This manipulation of the argument key1/key2/key3/key4/pskValue causes stack-based buffer overfl

9.8 **CVE-2017-20224** Telesquare sdt-cs3b1 firmware

Telesquare SKT LTE Router SDT-CS3B1 version 1.2.0 contains an arbitrary file upload vulnerability that allows unauthenticated attackers to upload malicious content by exploiting enabled WebDAV HTTP methods. Attackers can use PUT, DELETE, MKCOL, MOVE, COPY, and

9.8 **CVE-2026-4254** Tenda ac8 firmware

A weakness has been identified in Tenda AC8 up to 16.03.50.11. This vulnerability affects the function doSystemCmd of the file /goform/SysToolChangePwd of the component HTTP Endpoint. This manipulation of the argument local_2c causes stack-based buffer overflo

9.8 **CVE-2016-20026**
ZKTeco ZKBioSecurity 3.0 contains hardcoded credentials in the bundled Apache Tomcat server that allow unauthenticated attackers to access the manager application. Attackers can authenticate with hardcoded credentials stored in tomcat-users.xml to upload malic

9.8 **CVE-2016-20024**
ZKTeco ZKTime.Net 3.0.1.6 contains an insecure file permissions vulnerability that allows unprivileged users to escalate privileges by modifying executable files. Attackers can exploit world-writable permissions on the ZKTimeNet3.0 directory and its contents t

9.6 **CVE-2026-32626** Mintplexlabs anythingllm
AnythingLLM is an application that turns pieces of content into context that any LLM can use as references during chatting. In 1.11.1 and earlier, AnythingLLM Desktop contains a Streaming Phase XSS vulnerability in the chat rendering pipeline that escalates to

9.8 **CVE-2016-20030**
ZKTeco ZKBioSecurity 3.0 contains a user enumeration vulnerability that allows unauthenticated attackers to discover valid usernames by submitting partial characters via the username parameter. Attackers can send requests to the authLoginAction!login.do script

9.8 **CVE-2026-20998** Samsung smart switch
Improper authentication in Smart Switch prior to version 3.7.69.15 allows remote attackers to bypass authentication.

9.1 **CVE-2026-27962** Authlib authlib
Authlib is a Python library which builds OAuth and OpenID Connect servers. Prior to version 1.6.9, a JWK Header Injection vulnerability in authlib's JWS implementation allows an unauthenticated attacker to forge arbitrary JWT tokens that pass signature verific

9.8 **CVE-2025-69809** P2r3 bareiron
A write-what-where condition in p2r3 Bareiron commit 8e4d40 allows unauthenticated attackers to write arbitrary values to memory, enabling arbitrary code execution via a crafted packet.

11 more critical CVEs in this window: see the dashboard

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.