# Daily brief, Sunday, April 12, 2026

Apr 11, 8:00 PM to Apr 12, 8:00 PM ET

Generated Nov 7, 2026, 7:39 AM ET

| 0 | 0 | 0 | 8 | 0 | 1 |
|---|---|---|---|---|---|
| Breaking | Newly exploited | Exploit code | Critical CVEs | Ransomware posts | New breaches |

8 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

8

**9.8** **CVE-2026-6112**

A weakness has been identified in Totolink A7100RU 7.4cu.2313_b20191024. Affected is the function setRadvdCfg of the file /cgi-bin/cstecgi.cgi of the component CGI Handler. This manipulation of the argument maxRtrAdvInterval causes os command injection. The at

**9.8** **CVE-2026-6113**

A security vulnerability has been detected in Totolink A7100RU 7.4cu.2313_b20191024. Affected by this vulnerability is the function setTtyServiceCfg of the file /cgi-bin/cstecgi.cgi of the component CGI Handler. Such manipulation of the argument ttyEnable lead

**9.8** **CVE-2026-6114**

A vulnerability was detected in Totolink A7100RU 7.4cu.2313_b20191024. Affected by this issue is the function setNetworkCfg of the file /cgi-bin/cstecgi.cgi of the component CGI Handler. Performing a manipulation of the argument proto results in os command inj

9.8 **CVE-2026-6115**

A flaw has been found in Totolink A7100RU 7.4cu.2313_b20191024. This affects the function setAppCfg of the file /cgi-bin/cstecgi.cgi of the component CGI Handler. Executing a manipulation of the argument enable can lead to os command injection. The attack may

9.8 **CVE-2026-6116**

A vulnerability has been found in Totolink A7100RU 7.4cu.2313_b20191024. This vulnerability affects the function setDiagnosisCfg of the file /cgi-bin/cstecgi.cgi of the component CGI Handler. The manipulation of the argument ip leads to os command injection. R

9.8 **CVE-2019-25709** Codefuture image hosting script

CF Image Hosting Script 1.6.5 allows unauthenticated attackers to download and decode the application database by accessing the imgdb.db file in the upload/data directory. Attackers can extract delete IDs stored in plaintext from the deserialized database and

9.8 **CVE-2026-6131**

A vulnerability was found in Totolink A7100RU 7.4cu.2313_b20191024. Affected by this vulnerability is the function setTracerouteCfg of the file /cgi-bin/cstecgi.cgi of the component CGI Handler. The manipulation of the argument command results in os command in

9.8 **CVE-2026-6132**

A vulnerability was determined in Totolink A7100RU 7.4cu.2313_b20191024. Affected by this issue is the function setLedCfg of the file /cgi-bin/cstecgi.cgi of the component CGI Handler. This manipulation of the argument enable causes os command injection. Remot

## Ransomware

*No leak-site posts collected.*

## New data breaches 1

**Hallmark** hallmark.com 1,736,520 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. 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.