Daily brief, Thursday, June 18, 2026

Jun 17, 8:00 PM to Jun 18, 8:00 PM ET

Generated Nov 4, 2026, 7:02 PM ET

0	1	0	22	0	3
Breaking	Newly exploited	Exploit code	Critical CVEs	Ransomware posts	New breaches

1 newly exploited, 22 new critical CVEs, 3 new breaches.

Breaking

Nothing spreading fast in technology large companies run.

Newly exploited in the wild 1

9.8 **CVE-2026-20253** Splunk Enterprise CISA KEV DETECTION

An unauthenticated user creates or truncates arbitrary files with Splunk Enterprise.

New public exploit code

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

New critical CVEs 22

9.8 **CVE-2026-20253** Splunk Enterprise KEV EXPLOIT CODE DETECTION

An unauthenticated user creates or truncates arbitrary files with Splunk Enterprise.

9.8 **CVE-2026-54419** EXPLOIT CODE DETECTION

claudiopizzillo PIAF-HMS (PBX-In-A-Flash Hotel Management System; no released versions, latest commit 389d2633441b65ced1c104212cd62be2bfca21e5) contains multiple unauthenticated SQL injection vulnerabilities. The application has no authentication mechanism and

9.8 **CVE-2026-54130** Microsoft 365 copilot

Missing authentication for critical function in M365 Copilot allows an unauthorized attacker to disclose information over a network.

9.8 **CVE-2026-54390** JTL Software JTL Shop

JTL Shop versions 5.2.0 through 5.7.1 contains a server-side template injection vulnerability that allows unauthenticated attackers to inject malicious template syntax due to unsanitized user-supplied input passed to the Smarty template engine. Attackers can e

10.0 **CVE-2026-49257**

mcp-pinot is a Python-based Model Context Protocol (MCP) server for interacting with Apache Pinot. In versions 3.0.1 and below, mcp-pinot defaults to running an HTTP MCP server bound to 0.0.0.0:8080 with no authentication enabled. All MCP tools, including SQL

9.9 **CVE-2026-49252**

deepstream is a server that allows clients and backend services to sync data, send messages and make rpcs at scale. Versions prior to 10.0.5 are vulnerable to Prototype Pollution. Exploitation can lead to potential privilege escalation from any authenticated u

9.9 **CVE-2026-47647** Microsoft dynamics 365

Improper access control in Microsoft Dynamics 365 allows an authorized attacker to elevate privileges over a network.

9.8 **CVE-2026-55740**

Nur-Alam39 bus-ticket (no released versions; latest commit 459cabdbeb99c00225b26e46e3c2c30ae1de7bad) contains an unauthenticated SQL injection vulnerability in bus_info.php. The busid parameter received via HTTP POST is concatenated directly into a MySQL query

9.8 **CVE-2026-8024**

A remote, unauthenticated attacker may exploit a deserialization of untrusted data vulnerability in ibaPDA or ibaDatCoordinator to gain full access to the affected systems.

9.8 **CVE-2026-9158** Eclipse 4diac forte

In Eclipse 4diac FORTE versions 3.0.0 to 3.1.0, a specially crafted DELETE connection command to the management interface can lead to a dangling pointer. This allows subsequent commands to access freed memory (use-after-free).

9.8 **CVE-2026-38714** Inhandnetworks ir915l-fq39-s firmware

+3 more CVEs in the same release

InHand Networks IR912 V1.0.0.r20042 and IR915 V1.0.0.r20042 (including earlier versions) were discovered to contain a command injection vulnerability in the Python configuration function. This vulnerability allows remote attackers to execute arbitrary commands

9.8 **CVE-2026-54103**

The U.S. Government Accountability Office (GAO) Electronic Protest Docketing System (EPDS) and Civilian Board of Contract Appeals (CBCA) Electronic Docketing System (EDS) does not authenticate password change requests to the '/update-profile/N' API endpoint. A

9.8 **CVE-2026-47846**

Bitnami Cassandra container images are affected by a retained default superuser vulnerability. When a custom administrator account is configured via the CASSANDRA_USER environment variable, the container initialization script creates the new superuser account

9.6 **CVE-2026-55742**

Cotonti 1.0.0 (master branch, commit f43f1fc3) is vulnerable to Cross-Site Request Forgery in the administration rights handler. In system/admin/admin.rights.php, the rights update action ('a=update') modifies group access rights (including via cot_auth_add_gr

9.3 **CVE-2026-48768**

TypeBot is a chatbot builder tool. In versions 3.16.1 and earlier, POST /api/blocks/file-input/v3/generate-upload-url is unauthenticated and uses unsanitized fileName input to construct public/ S3 object keys, while issuing presigned PUT URLs that do not bind

9.3 **CVE-2025-10560**

Worksnaps before version 1.6.20260201 contains hardcoded cloud credentials and related secret material in the Worksnaps client application binaries. The exposed credentials included AWS access keys, S3 bucket names, and related cloud access information. The or

9.1 **CVE-2026-11717** Google mcp toolbox for databases

+1 more CVEs in the same release

An authentication bypass vulnerability exists in the generic opaque token validation path (validateOpaqueToken) of googleapis/mcp-toolbox. When verifying an unparsed opaque token via an OAuth 2.0 introspection endpoint (RFC 7662), the toolbox decodes the respo

9.1 **CVE-2026-49454**

Relyra is a strict-by-default SAML 2.0 Service Provider library for Elixir and Phoenix. Versions 1.0.0 and 1.1.0 accept forged SAML signatures because SignatureValue was not cryptographically verified before the library returned a successful authentication res

Ransomware

No leak-site posts collected.

New data breaches 3

Operation Endgame 4.0	4,348,526 accounts
CFGI cfgi.com	248,235 accounts
Ralph Lauren ralphlauren.com	139,903 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.