

Daily brief, Tuesday, October 20, 2026

Oct 19, 8:00 PM to Oct 20, 8:00 PM ET

Generated Oct 31, 2026, 12:18 AM ET

0

Breaking

6

Newly exploited

0

Exploit code

76

Critical CVEs

24

Ransomware posts

1

New breaches

6 newly exploited, 76 new critical CVEs, 24 ransomware posts, 1 new breaches.

Breaking

Nothing spreading fast in technology large companies run.

Newly exploited in the wild

6

7.8

CVE-2026-106931 EG Secure Solutions SiteGuard Server Edition CISA KEV

An attacker can execute arbitrary OS commands with root or SYSTEM privileges on EG Secure Solutions SiteGuard Server Edition.

7.2

CVE-2026-96656 Plex Media Server CISA KEV

An admin user can write arbitrary files that may be executed on load on Plex Media Server.

6.7

CVE-2026-110936 Siemens Software Center CISA KEV

Siemens Software Center contains an uncontrolled search path element vulnerability that could allow an authenticated local attacker to place a specially crafted DLL in a directory that the application searches, leading to arbitrary code execution with the priv

6.5

CVE-2026-96654 Plex Media Server CISA KEV DETECTION

An attacker can call other plugins' functions and supply their own parameters on Plex Media Server.

4.3

CVE-2026-96652 Plex Media Server CISA KEV DETECTION

An attacker with any X-Plex-Token value can force Plex Media Server to POST to an attacker's chosen destination.

4.3

CVE-2026-96655 Plex Media Server CISA KEV DETECTION

An authenticated attacker can request arbitrary internal or external addresses via Plex Media Server.

New public exploit code

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

New critical CVEs

76

10.0

CVE-2026-91221 Oracle Oracle SOA Suite**+7 more CVEs in the same release**

An attacker with network access can bypass authentication and compromise Oracle SOA Suite.

9.8

CVE-2026-91323 Oracle Oracle WebLogic Server**+1 more CVEs in the same release**

An attacker with HTTP access can bypass authentication and access Oracle WebLogic Server.

9.6

CVE-2026-113252 Google Chrome

A remote attacker can execute arbitrary code outside the sandbox via a crafted HTML page in Google Chrome on Windows.

9.8

CVE-2026-101767 Oracle Oracle Application Object Library

An attacker with network access can bypass authentication and access Oracle Application Object Library.

9.6

CVE-2026-113072 Google Chrome

A remote attacker can execute arbitrary code outside the sandbox via a crafted HTML page in Google Chrome.

10.0

CVE-2026-101809 Oracle Workflow

An attacker can bypass authentication and access Workflow.

9.8

CVE-2026-91233 Oracle soa suite

An unauthenticated attacker with network access via SOAP can bypass authentication and compromise Oracle SOA Suite.

9.9

CVE-2026-91250 Oracle Oracle SOA Suite**+2 more CVEs in the same release**

A low-privileged attacker with network access via multiple protocols can escalate privileges on Oracle SOA Suite.

10.0

CVE-2026-87337 Oracle Oracle Access Manager

An unauthenticated attacker with network access via HTTP can disclose sensitive information on Oracle Access Manager.

9.6

CVE-2026-113078 Google chrome

A remote attacker can execute arbitrary code outside the sandbox in Google Chrome.

10.0

CVE-2026-91299 Oracle JD Edwards EnterpriseOne Orchestrator

An attacker can bypass authentication and access JD Edwards EnterpriseOne Orchestrator.

9.9

CVE-2026-91638 Oracle Oracle Essbase**+5 more CVEs in the same release**

An attacker with network access via HTTP can bypass authentication and compromise Oracle Essbase.

9.8	CVE-2026-91490 Oracle identity manager connector +1 more CVEs in the same release An unauthenticated attacker with network access via LDAP can compromise Oracle Identity Manager Connector.
9.6	CVE-2026-87347 Oracle Oracle HTTP Server An attacker can obtain sensitive information from Oracle HTTP Server.
9.6	CVE-2026-101420 Oracle PeopleSoft Enterprise PeopleTools A low-privileged attacker can bypass authentication and access PeopleSoft Enterprise PeopleTools.
9.6	CVE-2026-91243 Oracle Oracle Business Process Management Suite An attacker can bypass authentication in Oracle Business Process Management Suite.
9.1	CVE-2026-91241 Oracle Oracle Business Intelligence Enterprise Edition An attacker with network access can bypass authentication in Oracle Business Intelligence Enterprise Edition.
9.1	CVE-2026-94265 Curl curl A malicious server can force curl to re-transmit authentication state for an arbitrary host.
9.9	CVE-2026-91354 Oracle Oracle Outside In Technology A low-privileged attacker with network access via HTTP can bypass access control on Oracle Outside In Technology.
9.1	CVE-2026-86413 Curl curl An attacker gets curl's credential details without authentication or user interaction.

40 more critical CVEs in this window: [see the dashboard](#)

Ransomware

24

24 victims posted to leak sites. Most active: Booba Project (6), N0n (5), SilentRansomGroup (3), payload (2), Mimori (2).

New data breaches

1

Assurance Retraite lassuranceretraite.fr	70,372 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.