Daily brief, Tuesday, November 18, 2025

Nov 17, 7:00 PM to Nov 18, 7:00 PM ET

Generated Nov 9, 2026, 8:27 AM ET

0	1	0	19	0	0
Breaking	Newly exploited	Exploit code	Critical CVEs	Ransomware posts	New breaches

1 newly exploited, 19 new critical CVEs.

Breaking

Nothing spreading fast in technology large companies run.

Newly exploited in the wild

1

6.7 **CVE-2025-58034** Fortinet FortiWeb CISA KEV DETECTION

An attacker can execute remote OS commands on Fortinet FortiWeb appliances through the web-based management interface, leading to full system compromise.

New public exploit code

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

New critical CVEs

19

9.1 **CVE-2025-40549** Solarwinds serv-u

A Path Restriction Bypass vulnerability exists in Serv-U that when abused, could give a malicious actor with access to admin privileges the ability to execute code on a directory. This issue requires administrative privileges to abuse. On Windows systems, this

9.1 **CVE-2025-40547** Solarwinds serv-u

A logic error vulnerability exists in Serv-U which when abused could give a malicious actor with access to admin privileges the ability to execute code. This issue requires administrative privileges to abuse. On Windows deployments, the risk is scored as a med

9.8 **CVE-2025-63228** Dbbroadcast mozart next 100 firmware

The Mozart FM Transmitter web management interface on version WEBMOZZI-00287, contains an unauthenticated file upload vulnerability in the /upload_file.php endpoint. An attacker can exploit this by sending a crafted POST request with a malicious file (e.g., a

10.0 **CVE-2025-63216** Itel idgateway firmware

The Itel DAB Gateway (IDGat build c041640a) is vulnerable to Authentication Bypass due to improper JWT validation across devices. Attackers can reuse a valid JWT token obtained from one device to authenticate and gain administrative access to any other device

9.1 **CVE-2025-40548** Solarwinds serv-u

A missing validation process exists in Serv U when abused, could give a malicious actor with access to admin privileges the ability to execute code. This issue requires administrative privileges to abuse. On Windows deployments, the risk is scored as a medium

9.8 **CVE-2025-41733** Metz-Connect ewio2-m firmware

The commissioning wizard on the affected devices does not validate if the device is already initialized. An unauthenticated remote attacker can construct POST requests to set root credentials.

9.8 **CVE-2025-63225** Eurolab-Srl elts 100 firmware

The Eurolab ELTS100_UBX device (firmware version ELTS100v1.UBX) is vulnerable to Broken Access Control due to missing authentication on critical administrative endpoints. Attackers can directly access and modify sensitive system and network configurations, upl

9.8 **CVE-2025-63217** Itel id mux firmware

The Itel DAB MUX (IDMUX build c041640a) is vulnerable to Authentication Bypass due to improper JWT validation across devices. Attackers can reuse a valid JWT token obtained from one device to authenticate and gain administrative access to any other device runn

9.8 **CVE-2025-41348** Iest winplus

SQL injection vulnerability in WinPlus v24.11.27 by Informática del Este. This vulnerability allows an attacker recover, create, update an delete databases by sendng a POST request using the parameters 'val1' and 'cont in '/WinplusPortal/ws/sWinplus.svc/json/g

9.8 **CVE-2025-41734** Metz-Connect ewio2-m firmware

An unauthenticated remote attacker can execute arbitrary php files and gain full access of the affected devices.

9.8 **CVE-2025-54321** Ascertia signinghub

In Ascertia SigningHub through 8.6.8, there is a lack of rate limiting on the reset password function, leading to an email bombing vulnerability. An authenticated attacker can exploit this by automating reset password requests.

9.0 **CVE-2025-64325** Emby emby

Emby Server is a personal media server. Prior to version 4.8.1.0 and prior to Beta version 4.9.0.0-beta, a malicious user can send an authentication request with a manipulated X-Emby-Client value, which gets added to the devices section of the admin dashboard

9.8 **CVE-2025-63695** Dzzoffice dzzoffice

DzzOffice v2.3.7 and before is vulnerable to Arbitrary File Upload in /dzz/system/ueditor/php/controller.php.

9.1 **CVE-2025-56643** Requarks wiki.js

Requarks Wiki.js 2.5.307 does not properly revoke or invalidate active JWT tokens when a user logs out. As a result, previously issued tokens remain valid and can be reused to access the system, even after logout. This behavior affects session integrity and ma

9.8 **CVE-2025-63694** Dzzoffice dzzoffice

DzzOffice v2.3.7 and before is vulnerable to SQL Injection in explorer/groupmanage.

9.8 **CVE-2025-41347** Iest winplus

Unlimited upload vulnerability for dangerous file types in WinPlus v24.11.27 from Informática del Este. This vulnerability allows an attacker to upload a 'webshell' by sending a POST request to '/WinplusPortal/ws/sWinplus.svc/json/uploadfile'.

9.8 **CVE-2025-41346** Iest winplus

Faulty authorization control in software WinPlus v24.11.27 by Informática del Este that allows another user to be impersonated simply by knowing their 'numerical ID', meaning that an attacker could compromise another user's account, thereby affecting the confi

9.4 **CVE-2025-12383** Eclipse Foundation Jersey

In Eclipse Jersey versions 2.45, 3.0.16, 3.1.9 a race condition can cause ignoring of critical SSL configurations - such as mutual authentication, custom key/trust stores, and other security settings. This issue may result in SSLHandshakeException under normal

9.8 **CVE-2025-9312** Wso2 api control plane

A missing authentication enforcement vulnerability exists in the mutual TLS (mTLS) implementation used by System REST APIs and SOAP services in multiple WSO2 products. Due to improper validation of client certificate–based authentication in certain default con

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.