



Daily Threat Bulletin

29 May 2026

Vulnerabilities

[CVE-2026-35616: FortiClient EMS Flaw Actively Exploited in Malware Attacks](#)

Security Affairs - 28 May 2026 17:05

A critical FortiClient Endpoint Management Server (EMS) vulnerability patched in April has been exploited in fresh attacks to deploy information-stealing malware, Arctic Wolf reports. The flaw, tracked as CVE-2026-35616 (CVSS score of 9.1), can be exploited remotely via crafted requests for remote code execution (RCE) and does not require authentication.

[Critical Gogs RCE Vulnerability Lets Any Authenticated User Execute Arbitrary Code](#)

The Hacker News - 28 May 2026 23:54

A critical security vulnerability has been disclosed in Gogs, a popular open-source self-hosted Git service, that allows an authenticated user to execute arbitrary code under certain conditions.

[Oracle May 2026 Critical Security Patch Update Addresses 35 CVEs](#)

Security Boulevard - 29 May 2026 04:06

The May 2026 Critical Security Patch Update (CSPU) contains fixes for 35 unique CVEs in 35 security updates, 11 issues (31.4% of all patches) were assigned a critical severity rating.

Threat actors and malware

[Google Unveils AI Threat Defense Platform to Fight AI-Powered Cyberattacks](#)

SecurityWeek - 28 May 2026 10:55

New AI Threat Defense platform combines capabilities from Mandiant, Wiz and Gemini to help customers fight AI with AI.

[Carnival Cruise confirms data breach affecting nearly 6 million people](#)

BleepingComputer - 28 May 2026 07:49

Carnival Corporation, the world's largest cruise line operator, has confirmed a data breach affecting nearly 6 million people claimed by the ShinyHunters extortion gang in April 2026.

[BTMOB Android malware service generates custom phishing payloads](#)

BleepingComputer - 28 May 2026 18:10

An Android remote access trojan named BTMOB is offered to cybercriminals with a builder interface for generating malware payloads tailored to phishing lures.



Scottish
Cyber
Coordination
Centre

GreyVibe hackers use ChatGPT, Gemini to power cyberattacks

BleepingComputer - 28 May 2026 19:24

A likely Russian threat cluster tracked as GreyVibe has been targeting Ukrainian entities with AI-generated lures and a rich set of custom malware tools.

Fake ChatGPT download site infects Windows and Mac users with malware

Malwarebytes - 28 May 2026 11:18

Searching for ChatGPT? This fake download site serves malware to both Windows and Mac users, using separate payloads tailored to each platform.

Attackers Move Past Typosquatting to Realistic Package Impersonation

Infosecurity Magazine - 28 May 2026 16:30

Most malicious open source packages now mimic real code rather than rely on typosquatting.

UK incidents

Russia conducting daily attacks on UK 'from seabed to cyberspace,' spy chief warns

The Record from Recorded Future News - 28 May 2026 14:20

The head of Britain's cyber and signals intelligence agency delivered a stark warning Wednesday that Russia is conducting daily hybrid attacks against the United Kingdom and Europe, stretching "from the seabed to cyberspace."