Scottish Cyber Coordination Centre

Daily Threat Bulletin

22 June 2026

Vulnerabilities

Hackers exploit info disclosure bug in Gravity SMTP WordPress plugin

BleepingComputer - 19 June 2026 17:25

Threat actors are exploiting an unauthenticated information disclosure vulnerability in the WordPress plugin Gravity SMTP, active on 100,000 sites. [...]

CISA Warns of Active Exploitation Following FortiBleed Leak

Security Affairs - 20 June 2026 09:10

FortiBleed exposed credentials for 74,000 Fortinet devices, with attackers actively exploiting the leak to target systems worldwide. On June 18, CISA issued an emergency alert after reports surfaced that credentials for approximately 74,000 Fortinet firewalls and VPN gateways had been leaked in what researchers are calling FortiBleed.

Unpatchable 'usbliter8' Exploit Breaks Apple A12 and A13 SecureROM Boot Chain

The Hacker News - 20 June 2026 01:07

Security researchers at Paradigm Shift have published a working exploit, dubbed usbliter8, that achieves arbitrary code execution inside the SecureROM of Apple's A12 and A13 chips.That code is burned into the silicon at manufacture.

AutoJack Attack Lets One Web Page Hijack AI Agent for Host Code Execution

The Hacker News - 19 June 2026 22:00

Microsoft researchers have detailed an exploit chain, named AutoJack, that turns an AI browsing agent into a delivery vehicle for remote code execution.Steer the agent to load an attacker's web page, and that page's JavaScript can reach a privileged local service on the same machine and spawn a process on the host.

CISA Adds One Known Exploited Vulnerability to Catalog

CISA Advisories -

CISA has added one new vulnerability to its Known Exploited Vulnerabilities (KEV) Catalog, based on evidence of active exploitation. CVE-2026-20253 Splunk Enterprise Missing Authentication for Critical Function.

Threat actors and malware

New Prinz Eugen ransomware prioritizes recent files for encryption

BleepingComputer - 20 June 2026 12:23

Scottish Cyber Coordination Centre

A new ransomware operation named ‘Prinz Eugen’ prioritizes recently modified files for encryption and leaves no ransom note on the system. [...]

Microsoft links Mastra AI supply chain attack to North Korean hackers

BleepingComputer - 20 June 2026 11:09

Microsoft has attributed a recent Mastra AI supply chain attack that compromised more than 140 npm packages to the North Korean hacking group Sapphire Sleet, also known as BlueNoroff. [...]

Klue OAuth breach victim list grows as Icarus hackers claim attack

BleepingComputer - 19 June 2026 19:31

Market intelligence platform Klue has publicly confirmed a recent security incident that allowed threat actors to steal OAuth tokens used to connect to customers’ Salesforce environments, as the new “Icarus” extortion group publicly claims the attack. [...]

The Gentlemen RaaS Uses GentleKiller EDR Framework Targeting 400 Security Processes

The Hacker News - 20 June 2026 01:03

The Gentlemen ransomware-as-a-service (RaaS) operation is actively developing and maintaining a suite of endpoint detection and response (EDR) killers that it hands out to affiliates for impairing system defenses before deploying the encryptor.This mature portfolio of EDR-terminating tools is centered around a framework that’s known as GentleKiller.