Scottish Cyber Coordination Centre

Daily Threat Bulletin

13 July 2026

Vulnerabilities

New U-Boot flaws could enable stealthy firmware attacks

BleepingComputer - 10 July 2026 18:59

Six vulnerabilities in the widely used U-Boot bootloader have been discovered that could allow attackers to execute malicious code during device boot, potentially enabling stealthy firmware attacks that compromise security protections and install persistent malware. [...]

Hackers exploit critical auth bypass in Gitea Docker image

BleepingComputer - 10 July 2026 12:48

Hackers are actively exploiting a critical vulnerability in the official Docker image for the Gitea self-hosted Git service that allows attackers to impersonate any user, including administrators. [...]

Update Now: Critical Zimbra Classic Web Client Flaw Could Expose Mailboxes

Security Affairs - 10 July 2026 21:42

Zimbra addressed a critical stored XSS vulnerability in its Classic Web Client that lets malicious emails execute code when opened. Zimbra has released version 10.1.19 to fix a critical stored XSS vulnerability in its Classic Web Client, which is widely used to access Zimbra Collaboration.

Unpatched XRING Flaw in XQUIC Lets Remote Clients Crash HTTP/3 Servers

The Hacker News - 10 July 2026 18:17

A single wrong variable on one line in XQUIC, Alibaba's QUIC and HTTP/3 library, lets any remote client crash the server with a short burst of completely legal traffic. There is no patch.FoxIO researcher Sébastien Féry disclosed the flaw on July 8 and nicknamed it XRING.

Two Chrome updates in two days fix critical vulnerabilities

Malwarebytes - 10 July 2026 11:32

Chrome updates are arriving within days of each other. Learn how to update Chrome and check if you're running the latest version.

CISA Adds Two Known Exploited Vulnerabilities to Catalog

CISA Advisories -

CISA has added two new vulnerabilities to its Known Exploited Vulnerabilities (KEV) Catalog, based on evidence of active exploitation.CVE-2026-48939 iCagenda Unrestricted Upload of

File with Dangerous Type Vulnerability. CVE-2026-56291 Balbooa Forms Unrestricted Upload of File with Dangerous Type Vulnerability.

Threat actors and malware

RedHook Android malware now uses Wireless ADB for shell access

BleepingComputer - 12 July 2026 11:27

A new version of the RedHook Android malware abuses the Android Wireless Debugging (Wireless ADB) mechanism in a novel way to gain shell-level privileges without requiring a computer connection. [...]

Australia warns of global campaign targeting vulnerable CMS platforms

BleepingComputer - 11 July 2026 11:18

The Australian Cyber Security Centre (ACSC) issued an alert about a global exploitation campaign targeting vulnerable content management systems (CMS) and plugins. [...]

New U-Boot flaws could enable stealthy firmware attacks

BleepingComputer - 10 July 2026 18:59

Six vulnerabilities in the widely used U-Boot bootloader have been discovered that could allow attackers to execute malicious code during device boot, potentially enabling stealthy firmware attacks that compromise security protections and install persistent malware. [...]

Progress urges ShareFile admins to shut down servers over “credible” threat

BleepingComputer - 10 July 2026 13:26

Progress Software is emailing ShareFile customers who use Storage Zone Controllers to immediately shut down their servers after identifying what it describes as a “credible external security threat” targeting the on-premises secure file-sharing software. [...]

Hackers exploit critical auth bypass in Gitea Docker image

BleepingComputer - 10 July 2026 12:48

Hackers are actively exploiting a critical vulnerability in the official Docker image for the Gitea self-hosted Git service that allows attackers to impersonate any user, including administrators. [...]

222 GitHub Repositories Linked to Fake Go Package Malware Operation

Security Affairs - 10 July 2026 11:22

Researchers uncovered 222 GitHub repositories spreading malware through fake Go packages, delivering loaders, stealers, RATs, and cryptominers.

Exposed Hacker Server Reveals WP-SHELLSTORM Backdooring Thousands of WordPress Sites

The Hacker News - 10 July 2026 18:00

Scottish Cyber Coordination Centre

A cybercrime crew left one of its own servers wide open on the internet for three weeks, and it exposed the operation's inner workings: the hacking tools, the activity logs, and target lists naming more than 1.4 million websites.

Destructive Windows backdoor stuffs multiple wipers and ransomware code into a single package

The Register - 10 July 2026 20:35

Microsoft says GigaWiper combines at least 3 malware families into one modular tool

GigaWiper Combines Multiple Malware for System-Level Sabotage

SecurityWeek - 10 July 2026 10:12

The backdoor's destructive capabilities include a standalone wiper, ransomware encryption, and a multi-pass wiping command.

New Ransomware Exploits Malicious Driver to Remove Cybersecurity Protections

Infosecurity Magazine - 10 July 2026 14:00

GodDamn ransomware uses remote desktop application to secretly move around networks and drop the malicious PoisonX kernel driver

UK related

NHS Warns Staff Over Unauthorized Access to Patient Data

Infosecurity Magazine - 10 July 2026 10:00

NHS tells staff they could face prison for "inappropriate" access to patients' medical records