Scottish Cyber Coordination Centre

# Daily Threat Bulletin

25 August 2026

## Vulnerabilities

### Exploited Zimbra Flaw Highlights Shrinking Window to Patch

darkreading - 24 August 2026 22:46

CISA has issued a three-day deadline for agencies to patch a Zimbra security vulnerability, CVE-2026-73570, which allows full takeover of a user's communications.

### 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-2026-21962 Oracle HTTP Server and Oracle Weblogic Server Proxy Plug-in Improper Access Control Vulnerability

### Unpatched Calix flaw lets hackers bypass NAT to expose internal devices

BleepingComputer - 24 August 2026 18:14

An unpatched vulnerability in Calix GS7 XGS (GS5239XG) residential routers used by multiple U.S. broadband providers allows remote, unauthenticated attackers to create port-forwarding rules that can expose local network devices to the public internet.

### Critical Keycloak Password Reset Flaw Could Let Unauthenticated Attackers Take Over Any Account

The Hacker News - 24 August 2026 18:26

Red Hat and the Keycloak project have released patches to address a critical security flaw in the open-source identity and access management server that could allow an unauthenticated remote attacker to take over any user account by forcing a password reset.

## Threat actors and malware

### Hackers target WordPress sites in miniOrange auth bypass attacks

BleepingComputer - 24 August 2026 16:26

Hackers are attempting to exploit two critical authentication bypass vulnerabilities in the miniOrange SAML 2.0 Single Sign On plugin for WordPress that can be used to forge SAML responses and log in as administrators.

Scottish Cyber Coordination Centre

### Tricky 'SynkLoader' Multitool May Herald Ransomware

darkreading - 24 August 2026 16:02

An advanced, multilingual malware family brings back a trick from yesteryear — screen hijacking — for effective password theft, along with a slew of novel features.

### ToxicPanda Banking Trojan Matures Into Enterprise Threat

darkreading - 24 August 2026 15:34

The latest version of the Android malware has new features that expand its global reach and put more than users' financial applications at risk.

### Hackers infecting Android car systems to build proxy botnet

The Record from Recorded Future News - 24 August 2026 13:15

A new malware is being used to infect Android-based car systems, turning the devices into part of a botnet, researchers warned in a report published Friday.

## UK incidents

### US sanctions Iranian cyber actors as UK discloses power plant attack

The Record from Recorded Future News -

The U.S. sanctioned several Iranian nationals on Monday for cyberattacks on critical infrastructure just days after reports emerged of a cyber intrusion on a small power plant in the United Kingdom.