



Scottish  
Cyber  
Coordination  
Centre

# Daily Threat Bulletin

5 June 2025

## Vulnerabilities

### [Cisco warns of ISE and CCP flaws with public exploit code](#)

BleepingComputer - 04 June 2025 16:19

Cisco has released patches to address three vulnerabilities with public exploit code in its Identity Services Engine (ISE) and Customer Collaboration Platform (CCP) solutions.

### [Google fixes another actively exploited vulnerability in Chrome, so update now!](#)

Malwarebytes - 04 June 2025 16:18

Google has released an important update for Chrome, patching one actively exploited zero-day and two other security flaws

### [35K Solar Devices Vulnerable to Potential Hijacking](#)

darkreading - 04 June 2025 22:53

A new analysis shows that roughly 35,000 solar power systems from 42 vendors have exposed management interfaces, including devices such as inverters, data loggers, monitors, gateways, and more.

## Threat actors and malware

### [Thousands Hit by The North Face Credential Stuffing Attack](#)

SecurityWeek - 04 June 2025 10:53

Threat actors steal personal information from thenorthface.com user accounts in a recent credential stuffing campaign.

### [Google Warns of Vishing, Extortion Campaign Targeting Salesforce Customers](#)

SecurityWeek - 04 June 2025 15:00

A threat actor specializing in voice phishing (vishing) attacks is targeting Salesforce customers in a large-scale data theft and extortion campaign.

### [Chaos RAT Malware Targets Windows and Linux via Fake Network Tool Downloads](#)

The Hacker News - 04 June 2025 19:25

Threat hunters are calling attention to a new variant of a remote access trojan (RAT) called Chaos RAT that has been used in recent attacks targeting Windows and Linux systems.



Scottish  
Cyber  
Coordination  
Centre

### **Ramnit Malware Infections Spike in OT as Evidence Suggests ICS Shift**

SecurityWeek - 04 June 2025 12:04

Industrial giant Honeywell has published its 2025 Cybersecurity Threat Report with information on the latest trends.

### **FBI: Play ransomware breached 900 victims, including critical orgs**

BleepingComputer - 04 June 2025 17:06

In an update to a joint advisory with CISA and the Australian Cyber Security Centre, the FBI said that the Play ransomware gang had breached roughly 900 organizations as of May 2025, three times the number of victims reported in October 2023.

### **Ukraine's military intelligence claims cyberattack on Russian strategic bomber maker**

The Record from Recorded Future News - 04 June 2025 15:24

Ukraine's military intelligence agency (HUR) said it hacked into the internal systems of Russia's major state-owned aircraft manufacturer Tupolev, days after Ukraine launched surprise drone assaults on Russian air bases.

## **UK incidents**

### **#Infosec2025: UK Retail Hack Was 'Subtle, Not Complex,' Says River Island CISO**

Infosecurity Magazine - 04 June 2025 14:00

The attacks on UK retailers are "a wake-up call" for the industry, said River Island's Information Security Officer