Scottish Cyber Coordination Centre

# Daily Threat Bulletin

7 October 2025

## Vulnerabilities

### Oracle Rushes Patch for CVE-2025-61882 After Cl0p Exploited It in Data Theft Attacks

The Hacker News - 06 October 2025 18:07

Oracle has released an emergency update to address a critical security flaw in its E-Business Suite software that it said has been exploited in the recent wave of Cl0p data theft attacks.The vulnerability, tracked as CVE-2025-61882 (CVSS score: 9.8), concerns an unspecified bug that could allow an unauthenticated attacker with network access via HTTP to compromise and take control of the Oracle

### Redis warns of critical flaw impacting thousands of instances

BleepingComputer - 06 October 2025 12:55

The Redis security team has released patches for a maximum severity vulnerability that could allow attackers to gain remote code execution on thousands of vulnerable instances. [...]

### CISA Adds Seven Known Exploited Vulnerabilities to Catalog

CISA Advisories -

CISA has added seven new vulnerabilities to its Known Exploited Vulnerabilities (KEV) Catalog, based on evidence of active exploitation: CVE-2010-3765 Mozilla Multiple Products Remote Code Execution Vulnerability; CVE-2010-3962 Microsoft Internet Explorer Uninitialized Memory Corruption Vulnerability; CVE-2011-3402 Microsoft Windows Remote Code Execution Vulnerability; CVE-2013-3918 Microsoft Windows Out-of-Bounds Write VulnerabilityCVE-2021-22555 Linux Kernel Heap Out-of-Bounds Write Vulnerability; CVE-2021-43226 Microsoft Windows Privilege Escalation VulnerabilityCVE-2025-61882 Oracle E-Business Suite Unspecified Vulnerability.

## Threat actors and malware

### Microsoft: Critical GoAnywhere bug exploited in ransomware attacks

BleepingComputer - 06 October 2025 15:11

A cybercrime group, tracked as Storm-1175, has been actively exploiting a maximum severity GoAnywhere MFT vulnerability in Medusa ransomware attacks for nearly a month. [...]

### XWorm malware resurfaces with ransomware module, over 35 plugins

BleepingComputer - 06 October 2025 08:42

New versions of the XWorm backdoor are being distributed in phishing campaigns after the original developer, XCoder, abandoned the project last year. [...]

Scottish Cyber Coordination Centre

### Oracle patches critical E-Business Suite flaw exploited by Cl0p hackers

Security Affairs - 06 October 2025 14:39

Oracle fixed a critical flaw (CVE-2025-61882, CVSS 9.8) in E-Business Suite that is actively exploited by Cl0p cybercrime group.

### Zimbra users targeted in zero-day exploit using iCalendar attachments

Security Affairs - 06 October 2025 08:33

Threat actors exploited a Zimbra zero-day via malicious iCalendar (.ICS) files used to deliver attacks through calendar attachments. StrikeReady researchers discovered that threat actors exploited the vulnerability CVE-2025-27915 in Zimbra Collaboration Suite in zero-day attacks using malicious iCalendar (.ICS) files.

### Chinese Cybercrime Group Runs Global SEO Fraud Ring Using Compromised IIS Servers

The Hacker News - 06 October 2025 18:06

Cybersecurity researchers have shed light on a Chinese-speaking cybercrime group codenamed UAT-8099 that has been attributed to search engine optimization (SEO) fraud and theft of high-value credentials, configuration files, and certificate data.

## UK related

### FBI, UK gov't urge orgs to patch Oracle E-Business vuln after alleged Clop campaign

The Record from Recorded Future News - 06 October 2025 19:56

### CISA and UK NCSC Release Joint Guidance for Securing OT Systems

CISA Advisories -

CISA, in collaboration with the Federal Bureau of Investigation, the United Kingdom's National Cyber Security Centre, and other international partners has released new joint cybersecurity guidance: Creating and Maintaining a Definitive View of Your Operational Technology (OT) Architecture.Building on the recent Foundations for OT Cybersecurity: Asset Inventory Guidance for Owners and Operators.