Scottish Cyber Coordination Centre

# Daily Threat Bulletin

31 March 2025

## Vulnerabilities

### Mozilla fixed critical Firefox vulnerability CVE-2025-2857

Security Affairs - 28 March 2025 10:51

Mozilla addressed a critical vulnerability, tracked as CVE-2025-2857, impacting its Firefox browser for Windows. Mozilla has released security updates to address a critical flaw, tracked as CVE-2025-2857, impacting its Firefox browser for Windows. Recently, Google addressed a similar vulnerability, tracked as CVE-2025-2783, in Chrome that has been actively exploited in the wild as a zero-day. [...]

### RESURGE Malware Exploits Ivanti Flaw with Rootkit and Web Shell Features

The Hacker News - 30 March 2025 11:37

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) has shed light on a new malware called RESURGE that has been deployed as part of exploitation activity targeting a now-patched security flaw in Ivanti Connect Secure (ICS) appliances."RESURGE contains capabilities of the SPAWNCHIMERA malware variant, including surviving reboots; however, RESURGE contains distinctive commands that

### Vulnerability in most browsers abused in targeted attacks

Malwarebytes - 28 March 2025 17:46

A vulnerability has been found that can be exploited through every browser as long as its running on a Windows system

## Threat actors and malware

### CISA warns of RESURGE malware exploiting Ivanti flaw

Security Affairs - 31 March 2025 00:11

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) warns of RESURGE malware, targeting a vulnerability in Ivanti Connect Secure (ICS) appliances. The U.S. Cybersecurity and Infrastructure Security Agency (CISA) published a Malware Analysis Report (MAR) on a new malware called RESURGE. The malicious code has been used in attacks targeting the flaw CVE-2025-0282 in Ivanti Connect [...]

### BlackLock Ransomware Exposed After Researchers Exploit Leak Site Vulnerability

The Hacker News - 29 March 2025 10:22

In what's an instance of hacking the hackers, threat hunters have managed to infiltrate the online infrastructure associated with a ransomware group called BlackLock, uncovering crucial information about their modus operandi in the process. Resecurity said it identified a

security vulnerability in the data leak site (DLS) operated by the e-crime group that made it possible to extract

### Critical Condition: Legacy Medical Devices Remain Easy Targets for Ransomware

SecurityWeek - 28 March 2025 13:36

Analysis found that 99% of healthcare organizations are vulnerable to publicly available exploits.

## UK related

### Cardiff's children's chief confirms data leak 2 months after cyber risk was 'escalated'

The Register - 28 March 2025 13:28

Department director admits Welsh capital's council still trying to get heads around threat of dark web leaks Cardiff City Council's director of children's services says data was leaked or stolen from the organization, although she did not clarify how or what was pilfered....