Scottish Cyber Coordination Centre

# Daily threat bulletin

30 July 2024

## Vulnerabilities

### Acronis Cyber Infrastructure bug actively exploited in the wild

Security Affairs - 29 July 2024 16:16

Acronis warns of a critical vulnerability in its Acronis Cyber Infrastructure (ACI) solution that is being actively exploited in the wild. Acronis is warning of a critical vulnerability, tracked as CVE-2023-45249 (CVSS score of 9.8), in its Acronis Cyber Infrastructure (ACI) solution that is being actively exploited in the wild. ACI is a comprehensive IT [...]

### VMware ESXi Flaw Exploited by Ransomware Groups for Admin Access

The Hacker News - 30 July 2024 10:50

A recently patched security flaw impacting VMware ESXi hypervisors has been actively exploited by "several" ransomware groups to gain elevated permissions and deploy file-encrypting malware.The attacks involve the exploitation of CVE-2024-37085 (CVSS score: 6.8), an Active Directory integration authentication bypass that allows an attacker to obtain administrative access to the host.

### Millions of Websites Susceptible to XSS Attack via OAuth Implementation Flaw

SecurityWeek - 29 July 2024 13:00

Researchers discovered and published details of an XSS attack that could potentially impact millions of websites around the world.

## Threat actors and malware

### Proofpoint settings exploited to send millions of phishing emails daily

BleepingComputer - 29 July 2024 10:51

A massive phishing campaign dubbed "EchoSpoofing" exploited a security gap in Proofpoint's email protection service to dispatch millions of spoofed emails impersonating big entities like Disney, Nike, IBM, and Coca-Cola, to target Fortune 100 companies.

### Heimdal Security Presents its Latest Report on Brute-Force Cyberattacks

darkreading - 29 July 2024 22:18

### 'Zeus' Hacker Group Strikes Israeli Olympic Athletes in Data Leak

darkreading - 29 July 2024 19:04

Security presence has been heightened in Paris to ensure that the Games are safe, and Israeli athletes have been provided with even more protection.

Scottish
Cyber
Coordination
Centre