Scottish Cyber Coordination Centre

Daily threat bulletin

5 June 2024

Vulnerabilities

TikTok fixes zero-day bug used to hijack high-profile accounts

BleepingComputer - 04 June 2024 18:57

Over the past week, attackers have hijacked high-profile TikTok accounts belonging to multiple companies and celebrities, exploiting a zero-day vulnerability in the social media's direct messages feature.

Oracle WebLogic Server OS Command Injection Flaw Under Active Attack

The Hacker News - 04 June 2024 09:55

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) on Thursday added a security flaw impacting the Oracle WebLogic Server to the Known Exploited Vulnerabilities (KEV) catalog, citing evidence of active exploitation.

Cox Biz Auth-Bypass Bug Exposes Millions of Devices to Takeover

darkreading - 04 June 2024 15:06

The US broadband provider fixed an issue that allowed attackers to gain access to business customers' modems, and then access info and execute commands with the same permissions of an ISP support team.

Details of Atlassian Confluence RCE Vulnerability Disclosed

SecurityWeek - 04 June 2024 14:35

SonicWall has shared technical details on a recently addressed high-severity remote code execution flaw in Confluence. The post Details of Atlassian Confluence RCE Vulnerability Disclosed appeared first on SecurityWeek.

37 Vulnerabilities Patched in Android

SecurityWeek - 04 June 2024 09:49

Android's June 2024 security update resolves 37 vulnerabilities, including high-severity flaws in Framework and System. The post 37 Vulnerabilities Patched in Android appeared first on SecurityWeek.

Threat actors and malware

New V3B phishing kit targets customers of 54 European banks

BleepingComputer - 04 June 2024 15:53

Cybercriminals are promoting a new phishing kit named ‘V3B’ on Telegram, which currently targets customers of 54 major financial institutes in Ireland, the Netherlands, Finland, Austria, Germany, France, Belgium, Greece, Luxembourg, and Italy.

Hackers Use MS Excel Macro to Launch Multi-Stage Malware Attack in Ukraine

The Hacker News - 04 June 2024 17:37

A new sophisticated cyber attack has been observed targeting endpoints geolocated to Ukraine with an aim to deploy Cobalt Strike and seize control of the compromised hosts.The attack chain, per Fortinet FortiGuard Labs, involves a Microsoft Excel file that carries an embedded VBA macro to initiate the infection.

Russian Threat Groups Turn Eyes to the Paris Olympic Games

Security Boulevard - 04 June 2024 20:11

Russian threat groups are using old tactics and generative AI to run malicious disinformation campaigns meant to discredit the Paris Olympic Games, France and its president, and the IOC – less than two months before the Games begin.The post Russian Threat Groups Turn Eyes to the Paris Olympic Games appeared first on Security Boulevard.

Pentagon ‘doubling down’ on Microsoft despite ‘massive hack,’ senators complain

The Register - 04 June 2024 19:42

Meanwhile Mr Smith goes to Washington to testify before Congress The Pentagon is “doubling down” on its investment in Microsoft products despite the serious failings at the IT giant that put America’s national security at risk, say two US senators.

London Hospitals Cancel Operations Following Ransomware Incident

Infosecurity Magazine - 04 June 2024 17:41

A ransomware attack on a supplier of pathology services has forced leading London hospitals to cancel operations and divert emergency patients.