Scottish Cyber Coordination Centre

Daily threat bulletin

13 May 2024

Vulnerabilities

Chrome Zero-Day Alert — Update Your Browser to Patch New Vulnerability

The Hacker News - 10 May 2024 16:53

Google on Thursday released security updates to address a zero-day flaw in Chrome that it said has been actively exploited in the wild. Tracked as CVE-2024-4671, the high-severity vulnerability has been described as a case of use-after-free in the Visuals component.

Millions of IoT Devices at Risk from Flaws in Integrated Cellular Modem

darkreading - 10 May 2024 22:31

Researchers discovered seven vulnerabilities — including an unauthenticated RCE issue — in widely deployed Telit Cinterion modems.

Threat actors and malware

Pro-Russia hackers targeted Kosovo's government websites

Security Affairs - 12 May 2024 17:42

Pro-Russia hackers targeted government websites in Kosovo in retaliation for the government's support to Ukraine with military equipment. Pro-Russia hackers targeted Kosovo government websites, including the websites of the president and prime minister, with DDoS attacks.

Notorius threat actor IntelBroker claims the hack of the Europol

Security Affairs - 11 May 2024 16:01

Notorius threat actor IntelBroker claims that Europol has suffered a data breach that exposed FOUO and other classified data. The threat actor IntelBroker announced on the cybercrime forum Breach the hack of the European law enforcement agency Europol.

FIN7 Hacker Group Leverages Malicious Google Ads to Deliver NetSupport RAT

The Hacker News - 11 May 2024 13:59

The financially motivated threat actor known as FIN7 has been observed leveraging malicious Google ads spoofing legitimate brands as a means to deliver MSIX installers that culminate in the deployment of NetSupport RAT."

North Korean Hackers Deploy New Golang Malware 'Durian' Against Crypto Firms

The Hacker News - 10 May 2024 21:24

The North Korean threat actor tracked as Kimsuky has been observed deploying a previously undocumented Golang-based malware dubbed Durian as part of highly-targeted cyber attacks aimed at two South Korean cryptocurrency firms."Durian boasts comprehensive backdoor functionality, enabling the execution of delivered commands, additional file downloads, and exfiltration of files."

Healthcare Giant Ascension Hacked, Hospitals Diverting Emergency Service

SecurityWeek - 10 May 2024 14:33

One of the largest healthcare systems in the United States is scrambling to contain a hack that's causing disruption and "downtime procedures" at hospitals around the country.The post Healthcare Giant Ascension Hacked, Hospitals Diverting Emergency Service appeared first on SecurityWeek.

As of May 2024, Black Basta ransomware affiliates hacked over 500 organizations worldwide

Security Affairs - 12 May 2024 10:16

Black Basta ransomware affiliates have breached over 500 organizations between April 2022 and May 2024, FBI and CISA reported. The FBI, CISA, HHS, and MS-ISAC have issued a joint Cybersecurity Advisory (CSA) regarding the Black Basta ransomware activity as part of the StopRansomware initiative.