Scottish Cyber Coordination Centre

Daily threat bulletin

4 April 2024

Vulnerabilities

Google fixes two Pixel zero-day flaws exploited by forensics firms

BleepingComputer - 03 April 2024 11:47

Google has fixed two Google Pixel zero-days exploited by forensic firms to unlock phones without a PIN and gain access to the data stored within them. [...]

Ivanti Rushes Patches for 4 New Flaw in Connect Secure and Policy Secure

The Hacker News - 04 April 2024 11:15

Ivanti has released security updates to address four security flaws impacting Connect Secure and Policy Secure Gateways that could result in code execution and denial-of-service (DoS).The list of flaws is as follows -CVE-2024-21894 (CVSS score: 8.2) - A heap overflow vulnerability in the IPSec component of Ivanti Connect Secure (9.x, 22.x) and Ivanti Policy Secure allows an

Critical Vulnerability Found in LayerSlider Plugin Installed on a Million WordPress Sites

SecurityWeek - 03 April 2024 13:27

A critical SQL injection vulnerability in the LayerSlider WordPress plugin allows attackers to extract sensitive information.The post Critical Vulnerability Found in LayerSlider Plugin Installed on a Million WordPress Sites appeared first on SecurityWeek.

Google patches critical vulnerability for Androids with Qualcomm chips

Malwarebytes - 03 April 2024 21:40

Google has issued patches for 28 security vulnerabilities, including a critical patch for Androids with Qualcomm chips.

Threat actors and malware

Hosting firm's VMware ESXi servers hit by new SEXi ransomware

BleepingComputer - 03 April 2024 18:58

Scottish Cyber Coordination Centre

Chilean data center and hosting provider IxMetro Powerhost has suffered a cyberattack at the hands of a new ransomware gang known as SEXi, which encrypted the company's VMware ESXi servers and backups. [...]

The New Version of JsOutProx is Attacking Financial Institutions in APAC and MENA via Gitlab Abuse

Security Affairs - 03 April 2024 17:47

Resecurity researchers warn that a new Version of JsOutProx is targeting financial institutions in APAC and MENA via Gitlab abuse. Resecurity has detected a new version of JSOutProx, which is targeting financial services and organizations in the APAC and MENA regions. JSOutProx is a sophisticated attack framework utilizing both JavaScript and .NET. It employs the [...]

Mispadu Trojan Targets Europe, Thousands of Credentials Compromised

The Hacker News - 03 April 2024 16:02

The banking trojan known as Mispadu has expanded its focus beyond Latin America (LATAM) and Spanish-speaking individuals to target users in Italy, Poland, and Sweden.Targets of the ongoing campaign include entities spanning finance, services, motor vehicle manufacturing, law firms, and commercial facilities, according to Morphisec."Despite the geographic expansion, Mexico remains the

Scathing Federal Report Rips Microsoft for Shoddy Security, Insincerity in Response to Chinese Hack

SecurityWeek - 03 April 2024 14:08

Cyber Safety Review Board, said "a cascade of errors" by Microsoft let state-backed Chinese cyber operators break into email accounts of senior U.S. officials.The post Scathing Federal Report Rips Microsoft for Shoddy Security, Insincerity in Response to Chinese Hack appeared first on SecurityWeek.

RDP Abuse Present in 90% of Ransomware Breaches

Infosecurity Magazine - 03 April 2024 11:30

Sophos reveals "unprecedented" levels of RDP compromise in ransomware attacks in 2023