Scottish Cyber Coordination Centre

Daily threat bulletin

4 December 2024

Vulnerabilities

Exploit released for critical WhatsUp Gold RCE flaw, patch now

BleepingComputer - 03 December 2024 15:00

A proof-of-concept (PoC) exploit for a critical-severity remote code execution flaw in Progress WhatsUp Gold has been published, making it critical to install the latest security updates as soon as possible. [...]

Veeam warns of critical RCE bug in Service Provider Console

BleepingComputer - 03 December 2024 14:07

Veeam released security updates today to address two Service Provider Console (VSPC) vulnerabilities, including a critical remote code execution (RCE) discovered during internal testing. [...]

U.S. CISA adds ProjectSend, North Grid Proself, and Zyxel firewalls bugs to its Known Exploited Vulnerabilities catalog

Security Affairs - 04 December 2024 08:56

U.S. Cybersecurity and Infrastructure Security Agency (CISA) adds ProjectSend, North Grid Proself, and Zyxel firewalls bugs to its Known Exploited Vulnerabilities catalog. The U.S. Cybersecurity and Infrastructure Security Agency (CISA) added the following vulnerabilities to its Known Exploited Vulnerabilities (KEV) catalog: Proself versions before Ver5.62, Ver1.65, and Ver1.08 are vulnerable to XXE attacks, allowing unauthenticated attackers [...]

Critical SailPoint IdentityIQ Vulnerability Exposes Files to Unauthorized Access

The Hacker News - 04 December 2024 11:38

A critical security vulnerability has been disclosed in SailPoint's IdentityIQ identity and access management (IAM) software that allows unauthorized access to content stored within the application directory.The flaw, tracked as CVE-2024-10905, has a CVSS score of 10.0, indicating maximum severity. It affects IdentityIQ versions 8.2. 8.3, 8.4, and other previous versions.

Decade-Old Cisco Vulnerability Under Active Exploit

darkreading - 03 December 2024 21:25

Cisco encourages users to update to an unaffected version of its Adaptive Security Appliance (ASA) software since there are no workarounds for the 2014 vulnerability.

Threat actors and malware

Scottish Cyber Coordination Centre

CISA and Partners Release Joint Guidance on PRC-Affiliated Threat Actor Compromising Networks of Global Telecommunications Providers

CISA Advisories -

Today, CISA—in partnership with the National Security Agency (NSA), the Federal Bureau of Investigation (FBI), and international partners—released joint guidance, Enhanced Visibility and Hardening Guidance for Communications Infrastructure in response to a People's Republic of China (PRC)-affiliated threat actor's compromise of "networks of major global telecommunications providers to conduct a broad and significant cyber espionage campaign." The compromise of private communications impacted a limited number of individuals who are primarily involved in government or political activity.

Cloudflare's developer domains increasingly abused by threat actors

BleepingComputer - 03 December 2024 17:00

Cloudflare's 'pages.dev' and 'workers.dev' domains, used for deploying web pages and facilitating serverless computing, are being increasingly abused by cybercriminals for phishing and other malicious activities. [...]

Hackers Use Corrupted ZIPs and Office Docs to Evade Antivirus and Email Defenses

The Hacker News - 04 December 2024 11:18

Cybersecurity researchers have called attention to a novel phishing campaign that leverages corrupted Microsoft Office documents and ZIP archives as a way to bypass email defenses."The ongoing attack evades #antivirus software, prevents uploads to sandboxes, and bypasses Outlook's spam filters, allowing the malicious emails to reach your inbox," ANY.RUN said in a series of posts on X.

North Korean Kimsuky Hackers Use Russian Email Addresses for Credential Theft Attacks

The Hacker News - 03 December 2024 16:21

The North Korea-aligned threat actor known as Kimsuky has been linked to a series of phishing attacks that involve sending email messages that originate from Russian sender addresses to ultimately conduct credential theft."Phishing emails were sent mainly through email services in Japan and Korea until early September," South Korean cybersecurity company Genians said.

Horns&Hooves Campaign Delivers RATs via Fake Emails and JavaScript Payloads

The Hacker News - 03 December 2024 11:53

A newly discovered malware campaign has been found to target private users, retailers, and service businesses mainly located in Russia to deliver NetSupport RAT and BurnsRAT.The campaign, dubbed Horns&Hooves by Kaspersky, has hit more than 1,000 victims since it began around March 2023.

New phishing-as-a-service platform targets Microsoft 365

Security Magazine - 04 December 2024 01:00

Scottish Cyber Coordination Centre

New phishing-as-a-service platform steals Microsoft 365 credentials via large-scale adversary-in-the-middle attacks.

Venom Spider Spins Web of New Malware for MaaS Platform

darkreading - 03 December 2024 17:19

A novel backdoor malware and a loader that customizes payload names for each victim have been added to the threat group's cybercriminal tool set.

UK related

Severity of the risk facing the UK is widely underestimated, NCSC annual review warns

The Register - 03 December 2024 12:45

National cyber emergencies increased threefold this year The number of security threats in the UK that hit the country's National Cyber Security Centre's (NCSC) maximum severity threshold has tripled compared to the previous 12 months....