Scottish Cyber Coordination Centre

Daily threat bulletin

23 May 2024

Vulnerabilities

Critical Veeam Backup Enterprise Manager authentication bypass bug

Security Affairs - 22 May 2024 19:01

A critical security vulnerability in Veeam Backup Enterprise Manager could allow threat actors to bypass authentication. A critical vulnerability, tracked as CVE-2024-29849 (CVSS score: 9.8), in Veeam Backup Enterprise Manager could allow attackers to bypass authentication. Veeam Backup Enterprise Manager is a centralized management and reporting tool designed to simplify the administration of Veeam Backup & Replication [...]

Critical GitHub Enterprise Server Authentication Bypass bug. Fix it now!

Security Affairs - 22 May 2024 11:05

GitHub addressed a vulnerability in the GitHub Enterprise Server (GHES) that could allow an attacker to bypass authentication. GitHub has rolled out security fixes to address a critical authentication bypass issue, tracked as CVE-2024-4985 (CVSS score: 10.0), in the GitHub Enterprise Server (GHES).

GHOSTENGINE Exploits Vulnerable Drivers to Disable EDRs in Cryptojacking Attack

The Hacker News - 22 May 2024 15:27

Cybersecurity researchers have discovered a new cryptojacking campaign that employs vulnerable drivers to disable known security solutions (EDRs) and thwart detection in what's called a Bring Your Own Vulnerable Driver (BYOVD) attack.

MS Exchange Server Flaws Exploited to Deploy Keylogger in Targeted Attacks

The Hacker News - 22 May 2024 14:11

An unknown threat actor is exploiting known security flaws in Microsoft Exchange Server to deploy a keylogger malware in attacks targeting entities in Africa and the Middle East. Russian cybersecurity firm Positive Technologies said it identified over 30 victims spanning government agencies, banks, IT companies, and educational institutions.

QNAP Patches New Flaws in QTS and QuTS hero Impacting NAS Appliances

The Hacker News - 22 May 2024 11:45

Taiwanese company QNAP has rolled out fixes for a set of medium-severity flaws impacting QTS and QuTS hero, some of which could be exploited to achieve code execution on its network-attached storage (NAS) appliances.

Critical Netflix Genie Bug Opens Big Data Orchestration to RCE

darkreading - 22 May 2024 14:00

The severe security vulnerability (CVE-2024-4701, CVSS 9.9) gives remote attackers a way to burrow into Netflix's Genie open source platform, which is a treasure trove of information and connections to other internal services.

Ivanti Patches Critical Code Execution Vulnerabilities in Endpoint Manager

SecurityWeek - 22 May 2024 12:31

Ivanti has released product updates to resolve multiple vulnerabilities, including critical code execution flaws in Endpoint Manager. The post Ivanti Patches Critical Code Execution Vulnerabilities in Endpoint Manager appeared first on SecurityWeek.

Critical Vulnerability in Honeywell Virtual Controller Allows Remote Code Execution

SecurityWeek - 22 May 2024 12:15

Claroty shows how Honeywell ControlEdge Virtual UOC vulnerability can be exploited for unauthenticated remote code execution. The post Critical Vulnerability in Honeywell Virtual Controller Allows Remote Code Execution appeared first on SecurityWeek.

Chrome 125 Update Patches High-Severity Vulnerabilities

SecurityWeek - 22 May 2024 10:52

Google released a Chrome 125 update to resolve four high-severity vulnerabilities reported by external researchers.The post Chrome 125 Update Patches High-Severity Vulnerabilities appeared first on SecurityWeek.

UserPro Plugin Vulnerability Allows Account Takeover

Infosecurity Magazine - 22 May 2024 16:30

The plugin is used by over 20,000 sites and enables users to create customizable community websites

Threat actors and malware

Researchers Warn of Chinese-Aligned Hackers Targeting South China Sea Countries

The Hacker News - 22 May 2024 20:45

Cybersecurity researchers have disclosed details of a previously undocumented threat group called Unfading Sea Haze that’s believed to have been active since 2018.The intrusion singled out high-level organizations in South China Sea countries, particularly military and government targets, Bitdefender said in a report shared with The Hacker News.”The investigation revealed a troubling

Rockwell Advises Disconnecting Internet-Facing ICS Devices Amid Cyber Threats

The Hacker News - 22 May 2024 18:51

Rockwell Automation is urging its customers to disconnect all industrial control systems (ICSs) not meant to be connected to the public-facing internet to mitigate unauthorized or

malicious cyber activity.The company said it's issuing the advisory due to "heightened geopolitical tensions and adversarial cyber activity globally."To that end, customers are required to take immediate

Report Reveals 341% Rise in Advanced Phishing Attacks

Infosecurity Magazine - 22 May 2024 17:15

This data comes from SlashNext's mid-year State of Phishing 2024 report

UK Government in £8.5m Bid to Tackle AI Cyber-Threats

Infosecurity Magazine - 22 May 2024 10:15

The government is spending millions on research into AI safety