Scottish
Cyber
Coordination
Centre

Daily threat bulletin

22 May 2024

Vulnerabilities

GitHub warns of SAML auth bypass flaw in Enterprise Server

BleepingComputer - 21 May 2024 12:01

GitHub has fixed a maximum severity (CVSS v4 score: 10.0) authentication bypass vulnerability tracked as CVE-2024-4985, which impacts GitHub Enterprise Server (GHES) instances using SAML single sign-on (SSO) authentication. [...]

Critical Veeam Backup Enterprise Manager Flaw Allows Authentication Bypass

The Hacker News - 22 May 2024 10:15

Users of Veeam Backup Enterprise Manager are being urged to update to the latest version following the discovery of a critical security flaw that could permit an adversary to bypass authentication protections. Tracked as CVE-2024-29849 (CVSS score: 9.8),
the vulnerability could allow an unauthenticated attacker to log in to the Veeam Backup Enterprise Manager web interface.

Researchers Uncover Flaws in Python Package for AI Models and PDF.js Used by Firefox

The Hacker News - 21 May 2024 16:52

A critical security flaw has been disclosed in the llama_cpp_python Python package that could be exploited by threat actors to achieve arbitrary code execution.Tracked as CVE-2024-34359 (CVSS score: 9.7), the flaw has been codenamed Llama Drama by software supply chain security firm Checkmarx.

Critical Fluent Bit Bug Impacts All Major Cloud Platforms

Infosecurity Magazine - 21 May 2024 09:30

A newly discovered flaw in open source utility Fluent Bit could enable widespread DoS, RCE and information leakage.

Threat actors and malware

Malware Delivery via Cloud Services Exploits Unicode Trick to Deceive Users

The Hacker News - 21 May 2024 20:49

A new attack campaign dubbed CLOUD#REVERSER has been observed leveraging legitimate cloud storage services like Google Drive and Dropbox to stage malicious payloads."
The VBScript and PowerShell scripts in the CLOUD#REVERSER inherently involves

command-and-control-like activities by using Google Drive and Dropbox as staging platforms to manage file uploads and downloads."

SolarMarker Malware Evolves to Resist Takedown Attempts with Multi-Tiered Infrastructure

The Hacker News - 21 May 2024 19:37

The persistent threat actors behind the SolarMarker information-stealing malware have established a multi-tiered infrastructure to complicate law enforcement takedown efforts, new findings from Recorded Future show.

NextGen Healthcare Mirth Connect Under Attack - CISA Issues Urgent Warning

The Hacker News - 21 May 2024 13:43

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) on Monday added a security flaw impacting NextGen Healthcare Mirth Connect to its Known Exploited Vulnerabilities (KEV) catalog, citing evidence of active exploitation.