Scottish Cyber Coordination Centre

TLP CLEAR: Disclosure is not limited

Daily threat summary

27 March 2024

Vulnerabilities

Hackers exploit Ray framework flaw to breach servers, hijack resources

Bleeping Computer - March 26 2024

A new hacking campaign dubbed "ShadowRay" targets an unpatched vulnerability in Ray, a popular open-source AI framework, to hijack computing power and leak sensitive data from thousands of companies. According to a report by application security firm Oligo, these attacks have been underway since at least September 5, 2023, targeting education, cryptocurrency, biopharma, and other sectors.

Critical Flaw Found in D-Link Routers, Users Urged to Update

Cyber Security Asean - March 27 2024

A team of vulnerability researchers at Ensign InfoSecurity (“Ensign”), Asia’s largest cybersecurity service provider, discovered a zero-day vulnerability in D-Link DIR-822 router due to a stack-based buffer overflow vulnerability in the Home Network Administration Protocol service.

Apple Security Bug Opens iPhone, iPad to RCE

Dark Reading - March 26 2024

Apple finally has released more details on the mysterious updates the company silently pushed last week for iOS and iPadOS 17.4.1. As it turns out, the updates address a new vulnerability in the respective operating systems that allows a remote attacker to execute arbitrary code on affected iPhones and iPads.

Patch now: Mozilla patches two critical vulnerabilities in Firefox

Malwarebytes Labs Blog - March 26 2024

Mozilla released version 124.0.1 of the Firefox browser to Release channel users (the default channel that most non-developers run) on March 22, 2024. The new version fixes two critical security vulnerabilities. One of the vulnerabilities affects Firefox on desktop only, and doesn’t affect mobile versions of Firefox. Windows users that have automatic updates enabled should have the new version available as soon or shortly after they open the browser.

Scottish Cyber Coordination Centre

TLP CLEAR: Disclosure is not limited

Fortinet FortiClient EMS SQL injection flaw exploited in the wild
SC Magazine US - March 26 2024

Critical vulnerabilities in Fortinet FortiClient EMS, the Ivanti EPM Cloud Services Appliance, and the Nice Linear eMerge E-Series OS were added to the U.S. Cybersecurity and Infrastructure Agency's (CISA) Known Exploited Vulnerabilities (KEV) Catalog Monday. A high-severity vulnerability in Microsoft SharePoint Server was also added to the KEV database Tuesday.

Malware and threat actors

US, UK Accuse China of Years-Long Cyberespionage Campaign
Security Boulevard - RSS - March 26 2024

The United States, the UK, and other countries this week accused a state-sponsored Chinese threat group of running a massive global hacking campaign for more than a decade that targeted political figures, journalists, businesses, political dissidents, and...

Recent ‘MFA Bombing’ Attacks Targeting Apple Users
Krebs on Security - March 26 2024

Several Apple customers recently reported being targeted in elaborate phishing attacks that involve what appears to be a bug in Apple's password reset feature. In this scenario, a target's Apple devices are forced to display dozens of system-level prompts that prevent the devices from being used until the recipient responds "Allow" or "Don't Allow" to each prompt.

Threat actors use Tycoon 2FA kits to target MS 365 and Gmail accounts
MalwareTips.com - March 26 2024

Hackers use the phishing-as-a-service (PAAS) platform known as Tycoon 2FA to target Microsoft 365 and Gmail accounts. Their method bypasses two-factor authentication (2FA) systems. Also, the PAAS tool is similar to other Adversary-in-The-Middle (AiTM) phishing platforms such as Dadsec OTT.