Daily threat bulletin

17 September 2024

Vulnerabilities

Microsoft fixes bug crashing Microsoft 365 apps when typing

BleepingComputer - 16 September 2024 18:09

Microsoft has fixed a known issue that causes Microsoft 365 apps like Outlook, Word, Excel, and OneNote to crash while typing or spell-checking a text. [...]

CISA warns of Windows flaw used in infostealer malware attacks

BleepingComputer - 16 September 2024 16:53

CISA has ordered U.S. federal agencies to secure their systems against a recently patched Windows MSHTML spoofing zero-day bug exploited by the Void Banshee APT hacking group. [...]

D-Link fixes critical RCE, hardcoded password flaws in WiFi 6 routers

BleepingComputer - 16 September 2024 11:24

D-Link has fixed critical vulnerabilities in three popular wireless router models that allow remote attackers to execute arbitrary code or access the devices using hardcoded credentials. [...]

SolarWinds Issues Patch for Critical ARM Vulnerability Enabling RCE Attacks

The Hacker News - 17 September 2024 11:04

SolarWinds has released fixes to address two security flaws in its Access Rights Manager (ARM) software, including a critical vulnerability that could result in remote code execution.The vulnerability, tracked as CVE-2024-28991, is rated 9.0 out of a maximum of 10.0 on the CVSS scoring system.

Google Fixes GCP Composer Flaw That Could've Led to Remote Code Execution

The Hacker News - 16 September 2024 19:37

A now-patched critical security flaw impacting Google Cloud Platform (GCP) Composer could have been exploited to achieve remote code execution on cloud servers by means of a supply chain attack technique called dependency confusion.

Apple Patches Major Security Flaws With iOS 18 Refresh

SecurityWeek - 16 September 2024 20:06

Apple warns that attackers can use Siri to access sensitive user data, control nearby devices, or view recent photos without authentication.

CISA Adds Two Known Exploited Vulnerabilities to Catalog

CISA Advisories -

CISA has added two new vulnerabilities to its Known Exploited Vulnerabilities Catalog, based on evidence of active exploitation: CVE-2024-43461 Microsoft Windows MSHTML Platform Spoofing Vulnerability; CVE-2024-6670 Progress WhatsUp Gold SQL Injection Vulnerability.

CISA Adds One Known Exploited Vulnerability to Catalog

CISA Advisories -

CISA has added one new vulnerability to its Known Exploited Vulnerabilities Catalog, based on evidence of active exploitation: CVE-2024-8190 Ivanti Cloud Services Appliance OS Command Injection Vulnerability.

Threat actors and malware

CISA warns of Windows flaw used in infostealer malware attacks

BleepingComputer - 16 September 2024 16:53

CISA has ordered U.S. federal agencies to secure their systems against a recently patched Windows MSHTML spoofing zero-day bug exploited by the Void Banshee APT hacking group. [...]

Cyberattacks against manufacturing sector increased 105% in H1 of 2024

Security Magazine - 16 September 2024 13:00

New research shows how the cyber threat landscape is evolving, requiring greater proactive security strategies from organizations.

North Korean hacker group using false coding tests to spread malware

Security Magazine - 16 September 2024 09:00

Research has identified malicious software packages associated with the North Korean hacking group, Lazarus Group.

UK related

Half of UK Firms Lack Basic Cybersecurity Skills

Infosecurity Magazine - 16 September 2024 15:45

A new government report reveals that nearly half of UK businesses lack basic cybersecurity skills, while advanced skills like penetration testing and incident management are even more scarce.

Meta Goes Ahead With Controversial AI Training in UK

Infosecurity Magazine - 16 September 2024 10:15

Meta has unpaused a project to train AI on Facebook and Instagram posts, despite privacy concerns.