



Daily threat bulletin

3 September 2024

Vulnerabilities

[New Flaws in Microsoft macOS Apps Could Allow Hackers to Gain Unrestricted Access](#)

The Hacker News - 03 September 2024 10:31

Eight vulnerabilities have been uncovered in Microsoft applications for macOS that an adversary could exploit to gain elevated privileges or access sensitive data by circumventing the operating system's permissions-based model, which revolves around the Transparency, Consent, and Control (TCC) framework.

[Microsoft vulnerability that could enable data theft is now patched](#)

Security Magazine - 02 September 2024 09:00

Security leaders discuss a vulnerability in Microsoft 365 Copilot that was recently patched.

[Ubuntu Fixes Several Linux Kernel AWS Vulnerabilities](#)

Security Boulevard - 02 September 2024 10:00

Several vulnerabilities in the Linux kernel have been identified, also affecting Amazon Web Services (AWS) systems. Canonical has released important security patches addressing these vulnerabilities.

Threat actors and malware

[RansomHub Ransomware Group Targets 210 Victims Across Critical Sectors](#)

The Hacker News - 02 September 2024 20:03

Threat actors linked to the RansomHub ransomware group encrypted and exfiltrated data from at least 210 victims since its inception in February 2024, the U.S. government said.

[Cicada3301 Ransomware Group Emerges From the Ashes of ALPHV](#)

Infosecurity Magazine - 02 September 2024 10:15

Truesec claims new Cicada3301 ransomware-as-a-service group could have ties to ALPHV/BlackCat and Brutus.

UK related

[Transport for London \(TfL\) is dealing with an ongoing cyberattack](#)

Security Affairs - 02 September 2024 21:32



Scottish
Cyber
Coordination
Centre

Transport for London (TfL) is investigating an ongoing cyberattack. However, the TfL stated that there is no evidence that customer information was compromised during the incident. "We are currently dealing with an ongoing cyber security incident."