Scottish Cyber Coordination Centre

Daily threat bulletin

23 April 2024

Vulnerabilities

GitLab affected by GitHub-style CDN flaw allowing malware hosting

BleepingComputer - 22 April 2024 12:05

BleepingComputer recently reported how a GitHub flaw, or possibly a design decision, is being abused by threat actors to distribute malware using URLs associated with Microsoft repositories, making the files appear trustworthy. It turns out, GitLab is also affected by this issue and could be abused in a similar fashion. [...]

Russia-linked APT28 used post-compromise tool GooseEgg to exploit CVE-2022-38028 Windows flaw

Security Affairs - 22 April 2024 22:03

Russia-linked APT28 group used a previously unknown tool, dubbed GooseEgg, to exploit Windows Print Spooler service flaw. Microsoft reported that the Russia-linked APT28 group (aka “Forest Blizzard”, “Fancybear” or “Strontium” used a previously unknown tool, dubbed GooseEgg, to exploit the Windows Print Spooler flaw CVE-2022-38028.

Windows DOS-to-NT flaws exploited to achieve unprivileged rootkit-like capabilities

Security Affairs - 22 April 2024 11:25

Researcher demonstrated how to exploit vulnerabilities in the Windows DOS-to-NT path conversion process to achieve rootkit-like capabilities. SafeBreach researcher Or Yair devised a technique, exploiting vulnerabilities in the DOS-to-NT path conversion process, to achieve rootkit-like capabilities on Windows. When a user executes a function with a path argument in Windows, the DOS path of the [...]

Old Windows print spooler bug is latest target of Russia’s Fancy Bear gang

The Register - 23 April 2024 02:15

Putin’s pals use ‘GooseEgg’ malware to launch attacks you can defeat with patches or deletion Russian spies are exploiting a years-old Windows print spooler vulnerability and using a custom tool called GooseEgg to elevate privileges and steal credentials across compromised networks, according to Microsoft Threat Intelligence....

Scottish Cyber Coordination Centre

Threat actors and malware

Russian Sandworm hackers targeted 20 critical orgs in Ukraine

BleepingComputer - 22 April 2024 09:30

Russian hacker group Sandworm aimed to disrupt operations at around 20 critical infrastructure facilities in Ukraine, according to a report from the Ukrainian Computer Emergency Response Team (CERT-UA). [...]

ToddyCat Hacker Group Uses Advanced Tools for Industrial-Scale Data Theft

The Hacker News - 22 April 2024 21:41

The threat actor known as ToddyCat has been observed using a wide range of tools to retain access to compromised environments and steal valuable data.Russian cybersecurity firm Kaspersky characterized the adversary as relying on various programs to harvest data on an “industrial scale” from primarily governmental organizations.

MITRE Corporation Breached by Nation-State Hackers Exploiting Ivanti Flaws

The Hacker News - 22 April 2024 17:35

The MITRE Corporation revealed that it was the target of a nation-state cyber attack that exploited two zero-day flaws in Ivanti Connect Secure appliances starting in January 2024.The intrusion led to the compromise of its Networked Experimentation, Research, and Virtualization Environment (NERVE), an unclassified research and prototyping network.

Microsoft Warns: North Korean Hackers Turn to AI-Fueled Cyber Espionage

The Hacker News - 22 April 2024 13:42

Microsoft has revealed that North Korea-linked state-sponsored cyber actors have begun to use artificial intelligence (AI) to make its operations more effective and efficient.”They are learning to use tools powered by AI large language models (LLM) to make their operations more efficient and effective,” the tech giant said in its latest report on East Asia hacking groups.