Scottish Cyber Coordination Centre

Daily threat bulletin

14 October 2024

Vulnerabilities

NHS England Warns of Critical Veeam Vulnerability Under Active Exploitation

Infosecurity Magazine - 11 October 2024 16:00

NHS England has issued an alert regarding a critical Veeam Backup & Replication vulnerability that is being actively exploited, potentially leading to remote code execution.

Iranian hackers now exploit Windows flaw to elevate privileges

BleepingComputer - 13 October 2024 11:17

The Iranian state-sponsored hacking group APT34, aka OilRig, has recently escalated its activities with new campaigns targeting government and critical infrastructure entities in the United Arab Emirates and the Gulf region.

GitLab Patches Pipeline Execution, SSRF, XSS Vulnerabilities

SecurityWeek - 11 October 2024 10:37

The latest GitLab update resolves eight vulnerabilities, including critical- and high-severity pipeline execution flaws.

Threat actors and malware

US and UK govts warn: Russia scanning for your unpatched vulnerabilities

The Register - 12 October 2024 04:05

Also, phishing's easier over the phone, and your F5 cookies might be unencrypted, and more in brief If you need an excuse to improve your patching habits, a joint advisory from the US and UK governments about a massive, ongoing Russian campaign exploiting known vulnerabilities should do the trick.

GitHub, Telegram Bots, and ASCII QR Codes Abused in New Wave of Phishing Attacks

The Hacker News - 11 October 2024 23:43

A new tax-themed malware campaign targeting insurance and finance sectors has been observed leveraging GitHub links in phishing email messages as a way to bypass security measures and deliver Remcos RAT, indicating that the method is gaining traction among threat actors.

CISA Warns of Threat Actors Exploiting F5 BIG-IP Cookies for Network Reconnaissance

Scottish Cyber Coordination Centre

The Hacker News - 11 October 2024 15:04

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) is warning that it has observed threat actors leveraging unencrypted persistent cookies managed by the F5 BIG-IP Local Traffic Manager (LTM) module to conduct reconnaissance of target networks.It said the module is being used to enumerate other non-internet-facing devices on the network.

ShadowLogic Attack Targets AI Model Graphs to Create Codeless Backdoors

SecurityWeek - 11 October 2024 13:06

HiddenLayer details ShadowLogic, a new method of creating codeless backdoors in AI models by manipulating their graphs.

OpenAI confirms threat actors use ChatGPT to write malware

BleepingComputer - 12 October 2024 11:09

OpenAI has disrupted over 20 malicious cyber operations abusing its AI-powered chatbot, ChatGPT, for debugging and developing malware, spreading misinformation, evading detection, and conducting spear-phishing attacks.

INC ransomware rebrands to Lynx – same code, new name, still up to no good

The Register - 12 October 2024 00:00

Researchers point to evidence that scumbags visited the strategy boutique Researchers at Palo Alto's Unit 42 believe the INC ransomware crew is no more and recently rebranded itself as Lynx over a three-month period.