Scottish Cyber Coordination Centre

Daily threat bulletin

17 May 2024

Vulnerabilities

Researchers Uncover 11 Security Flaws in GE HealthCare Ultrasound Machines

The Hacker News - 16 May 2024 16:42

Security researchers have disclosed almost a dozen security flaws impacting the GE HealthCare Vivid Ultrasound product family that could be exploited by malicious actors to tamper with patient data and even install ransomware under certain circumstances."

The Fall of the National Vulnerability Database

darkreading - 16 May 2024 15:00

Since its inception, three key factors have affected the NVD's ability to classify security concerns — and what we're experiencing now is the result.

[R1] Nessus Agent Version 10.6.4 Fixes Multiple Vulnerabilities

Tenable Product Security Advisories - 16 May 2024 15:37

[R1] Nessus Agent Version 10.6.4 Fixes Multiple VulnerabilitiesArnie CabralThu, 05/16/2024 - 10:37 Two separate vulnerabilities were discovered, reported and fixed: When installing Nessus Agent to a directory outside of the default location on a Windows host, Nessus Agent versions prior to 10.6.4 did not enforce secure permissions for sub-directories. This could allow for local privilege escalation if users had not secured the directories in the non-default installation location

Threat actors and malware

Norway recommends replacing SSL VPN to prevent breaches

BleepingComputer - 16 May 2024 16:07

The Norwegian National Cyber Security Centre (NCSC) recommends replacing SSLVPN/WebVPN solutions with alternatives due to the repeated exploitation of related vulnerabilities in edge network devices to breach corporate networks. [...]

Russian hackers use new Lunar malware to breach a European govt's agencies

BleepingComputer - 16 May 2024 12:57

Security researchers discovered two previously unseen backdoors dubbed LunarWeb and LunarMail that were used to compromise a European government's diplomatic institutions abroad. [...]

Kimsuky hackers deploy new Linux backdoor in attacks on South Korea

BleepingComputer - 16 May 2024 10:28

The North Korean hacker group Kimsuki has been using a new Linux malware called Gomir that is a version of the GoBear backdoor delivered via trojanized software installers. [...]

North Korean Hackers Exploit Facebook Messenger in Targeted Malware Campaign

The Hacker News - 16 May 2024 20:18

The North Korea-linked Kimsuky hacking group has been attributed to a new social engineering attack that employs fictitious Facebook accounts to targets via Messenger and ultimately delivers malware."

Hackers Use Fake DocuSign Templates to Scam Organizations

Security Boulevard - 16 May 2024 22:30

Hackers can find templates for DocuSign and other companies for their phishing campaigns on dark web marketplaces for as little as $10.The post Hackers Use Fake DocuSign Templates to Scam Organizations appeared first on Security Boulevard.

SugarGh0st RAT Variant Used in Targeted AI Industry Attacks

Infosecurity Magazine - 16 May 2024 16:30

Proofpoint said the attackers modified registry key names for persistence