Scottish Cyber Coordination Centre

Daily threat bulletin

21 June 2024

Vulnerabilities

Phoenix UEFI vulnerability impacts hundreds of Intel PC models

BleepingComputer - 20 June 2024 18:31

A newly discovered vulnerability in Phoenix SecureCore UEFI firmware tracked as CVE-2024-0762 impacts devices running numerous Intel CPUs, with Lenovo already releasing new firmware updates to resolve the flaw.

CosmicSting flaw impacts 75% of Adobe Commerce, Magento sites

BleepingComputer - 20 June 2024 17:02

A vulnerability dubbed “CosmicSting” impacting Adobe Commerce and Magento websites remains largely unpatched nine days after the security update has been made available, leaving millions of sites open to catastrophic attacks.

SolarWinds Serv-U path traversal flaw actively exploited in attacks

BleepingComputer - 20 June 2024 12:45

Threat actors are actively exploiting a SolarWinds Serv-U path-traversal vulnerability, leveraging publicly available proof-of-concept (PoC) exploits.

An unpatched bug allows anyone to impersonate Microsoft corporate email accounts

Security Affairs - 20 June 2024 09:19

A researcher discovered a flaw that allows attackers to impersonate Microsoft corporate email accounts and launch phishing attacks. The security researcher Vsevolod Kokorin (@Slonser) discovered a bug that allows anyone to impersonate Microsoft corporate email accounts. An attacker can trigger the vulnerability to launch phishing attacks.

Atlassian Patches High-Severity Vulnerabilities in Confluence, Crucible, Jira

SecurityWeek - 20 June 2024 10:51

Atlassian has released Confluence, Crucible, and Jira updates to address multiple high-severity vulnerabilities.The post Atlassian Patches High-Severity Vulnerabilities in Confluence, Crucible, Jira appeared first on SecurityWeek.

Threat actors and malware

Linux version of RansomHub ransomware targets VMware ESXi VMs

BleepingComputer - 20 June 2024 16:00

The RansomHub ransomware operation is using a Linux encryptor designed specifically to encrypt VMware ESXi environments in corporate attacks. [...]

New Rust infostealer Fickle Stealer spreads through various attack methods

Security Affairs - 20 June 2024 14:08

New Rust-based Fickle Malware Uses PowerShell for UAC Bypass and Data Exfiltration A new Rust malware called Fickle Stealer spreads through various attack methods and steals sensitive information. Fortinet FortiGuard Labs researchers detected a new Rust-based information stealer called Fickle Stealer which spread through multiple attack vectors. The malware has an intricate code and relies on multiple [...]

LockBit Ransomware Again Most Active – Real Attack Surge or Smokescreen?

SecurityWeek - 20 June 2024 14:33

LockBit appears to once again be the most active ransomware group, but experts believe the hackers may just be inflating their numbers. The post LockBit Ransomware Again Most Active – Real Attack Surge or Smokescreen? appeared first on SecurityWeek.

UK incidents

Qilin: We knew our Synnovis attack would cause a healthcare crisis at London hospitals

The Register - 20 June 2024 11:29

Cybercriminals claim they used a zero-day to breach pathology provider's systems Interview The ransomware gang responsible for a healthcare crisis at London hospitals says it has no regrets about its cyberattack, which was entirely deliberate, it told The Register in an interview....