Scottish Cyber Coordination Centre

Daily threat bulletin

2 July 2024

Vulnerabilities

Cisco warns of NX-OS zero-day exploited to deploy custom malware

BleepingComputer - 01 July 2024 14:46

Cisco has patched an NX-OS zero-day exploited in April attacks to install previously unknown malware as root on vulnerable switches. [...]

Critical Flaws in CocoaPods Expose iOS and macOS Apps to Supply Chain Attacks

The Hacker News - 01 July 2024 22:42

A trio of security flaws has been uncovered in the CocoaPods dependency manager for Swift and Objective-C Cocoa projects that could be exploited to stage software supply chain attacks, putting downstream customers at severe risks.

New OpenSSH Vulnerability Could Lead to RCE as Root on Linux Systems

The Hacker News - 01 July 2024 17:20

OpenSSH maintainers have released security updates to contain a critical security flaw that could result in unauthenticated remote code execution with root privileges in glibc-based Linux systems.The vulnerability, codenamed regreSSHion, has been assigned the CVE identifier CVE-2024-6387.

'RegreSSHion' Bug Threatens Takeover of Millions of Linux Systems

darkreading - 01 July 2024 20:38

The high-severity CVE-2024-6387 in OpenSSH is a reintroduction of a 2006 flaw, and it allows unauthenticated RCE as root.

A Playbook for Detecting the OpenSSH Vulnerability – CVE-2024-6387 – regreSSHion

Security Boulevard - 01 July 2024 22:09

The Qualys Threat Research Unit has discovered a new "high" severity signal handler race condition vulnerability in OpenSSH's server software (sshd). According to the research, this vulnerability has the potential to allow remote unauthenticated code execution (RCE) for glibc-based Linux systems. This CVE has the potential to affect 14 million servers. Exploitation of this bug, [...]

Threat actors and malware

Latest Intel CPUs impacted by new Indirector side-channel attack

BleepingComputer - 01 July 2024 11:24

Modern Intel processors, including chips from the Raptor Lake and the Alder Lake generations are susceptible to a new type of a high-precision Branch Target Injection (BTI) attack dubbed 'Indirector,' which could be used to steal sensitive information from the CPU. [...]

CapraRAT Spyware Disguised as Popular Apps Threatens Android Users

The Hacker News - 01 July 2024 19:30

The threat actor known as Transparent Tribe has continued to unleash malware-laced Android apps as part of a social engineering campaign to target individuals of interest."These APKs continue the group's trend of embedding spyware into curated video browsing applications, with a new expansion targeting mobile gamers, weapons enthusiasts, and TikTok fans."

The Evolution of Phishing Attacks: Beyond Email and How to Protect Your Organization

Security Boulevard - 01 July 2024 17:57

The Evolution of Phishing Attacks: Beyond Email Phishing attacks have long been synonymous with email, but the landscape of cyberthreats has evolved dramatically. Today, phishing is not confined to email inboxes; it has permeated various communication channels, including SMS, WhatsApp, and collaboration tools like Microsoft Teams, Slack and Zoom.