Scottish Cyber Coordination Centre

Daily threat bulletin

16 April 2024

Vulnerabilities

Palo Alto Networks Releases Guidance for Vulnerability in PAN-OS, CVE-2024-3400

CISA Advisories -

Palo Alto Networks has released workaround guidance for a command injection vulnerability (CVE-2024-3400) affecting PAN-OS versions 10.2, 11.0, and 11.1. Palo Alto Networks has reported active exploitation of this vulnerability in the wild. CISA encourages users and administrators to review the Palo Alto Networks Security Advisory, apply the current mitigations, and update the affected software when Palo Alto Networks makes the fixes available. CISA has also added this vulnerability to its Known Exploited Vulnerabilities Catalog.

Intel and Lenovo BMCs Contain Unpatched Lighttpd Server Flaw

The Hacker News - 15 April 2024 23:21

A security flaw impacting the Lighttpd web server used in baseboard management controllers (BMCs) has remained unpatched by device vendors like Intel and Lenovo, new findings from Binarly reveal.

New LockBit Variant Exploits Self-Spreading Features

Infosecurity Magazine - 15 April 2024 16:30

Kaspersky also uncovered the use of the SessionGopher script to extract saved passwords.

Threat actors and malware

Cisco Duo's Multifactor Authentication Service Breached

darkreading - 15 April 2024 21:21

A third-party telephony service provider for Cisco Duo falls prey to social engineering, and the company advises customer vigilance against subsequent phishing attacks.

New SteganoAmor attacks use steganography to target 320 orgs globally

BleepingComputer - 15 April 2024 17:31

Scottish Cyber Coordination Centre

A new campaign conducted by the TA558 hacking group is concealing malicious code inside images using steganography to deliver various malware tools onto targeted systems. [...]

Muddled Libra Shifts Focus to SaaS and Cloud for Extortion and Data Theft Attacks

The Hacker News - 15 April 2024 19:59

The threat actor known as Muddled Libra has been observed actively targeting software-as-a-service (SaaS) applications and cloud service provider (CSP) environments in a bid to exfiltrate sensitive data."Organizations often store a variety of data in SaaS applications and use services from CSPs," Palo Alto Networks Unit 42 said in a report published last week."

Chipmaker Giant Nexperia Confirms Cyber-Attack Amid Ransomware Group Claims

Infosecurity Magazine - 15 April 2024 13:35

Nexperia confirmed its IT servers were accessed by attackers, with the Dunghill ransomware group claiming to have stolen chip designs and other sensitive documents