Scottish Cyber Coordination Centre

Daily threat bulletin

8 April 2024

Vulnerabilities

More than 16,000 Ivanti VPN gateways still vulnerable to RCE CVE-2024-21894

Security Affairs - 06 April 2024 17:54

Experts warn of roughly 16,500 Ivanti Connect Secure and Poly Secure gateways still vulnerable to a remote code execution (RCE) flaw. Shadowserver researchers reported that roughly 16,500 Ivanti Connect Secure and Poly Secure gateways are vulnerable to the recently reported RCE flaw CVE-2024-21894. This week the company released security updates to address four security flaws [...]

Cisco warns of XSS flaw in end-of-life small business routers

Security Affairs - 06 April 2024 09:22

Cisco warns customers of Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 Routers Cross-Site scripting flaw. Cisco warns of a Small Business RV016, RV042, RV042G, RV082, RV320, and RV325 routers Cross-Site scripting (XSS) flaw. The medium severity issue, tracked as CVE-2024-20362 (CVSS score 6.1), resides in the web-based management interface of Cisco Small Business [...]

Magento flaw exploited to deploy persistent backdoor hidden in XML

Security Affairs - 05 April 2024 21:41

Threat actors are exploiting critical Magento vulnerability CVE-2024-20720 to install a persistent backdoor on e-stores. Sansec researchers observed threat actors are exploiting the recently disclosed Magento vulnerability CVE-2024-20720 to deploy a persistent backdoor on e-stores. The vulnerability CVE-2024-20720 (CVSS score of 9.1) is an OS Command ('OS Command Injection') vulnerability that could lead to arbitrary code [...]

XZ-Utils Supply Chain Backdoor Vulnerability Updated Advisory (CVE-2024-3094)

Security Boulevard - 07 April 2024 09:23

Vulnerability Overview Recently, NSFOCUS CERT detected that the security community disclosed a supply chain backdoor vulnerability in XZ-Utils (CVE-2024-3094), with a CVSS score of 10. Since the underlying layer of SSH relies on liblzma, when certain conditions are met, an attacker can use this vulnerability to bypass SSH authentication and gain unauthorized access on the [...]The post XZ-Utils Supply Chain Backdoor Vulnerability Updated Advisory (CVE-2024-3094) appeared first on NSFOCUS, Inc., a global network and

cyber security leader, protects enterprises and carriers from advanced cyber attacks..The post XZ-Utils Supply Chain Backdoor Vulnerability Updated Advisory (CVE-2024-3094) appeared first on Security Boulevard.

Over 92,000 Internet-facing D-Link NAS devices can be easily hacked

Security Affairs - 07 April 2024 09:21

A researcher disclosed an arbitrary command injection and hardcoded backdoor issue in multiple end-of-life D-Link NAS models. A researcher who goes online with the moniker 'Netsecfish' disclosed a new arbitrary command injection and hardcoded backdoor flaw, tracked as , tracked as CVE-2024-3273, that impacts multiple end-of-life D-Link Network Attached Storage (NAS) device models. The flaw affects [...]

Threat actors and malware

US Health Dept warns hospitals of hackers targeting IT help desks

BleepingComputer - 06 April 2024 12:09

The U.S. Department of Health and Human Services (HHS) warns that hackers are now using social engineering tactics to target IT help desks across the Healthcare and Public Health (HPH) sector. [...]

Hackers Exploit Magento Bug to Steal Payment Data from E-commerce Websites

The Hacker News - 06 April 2024 16:13

Threat actors have been found exploiting a critical flaw in Magento to inject a persistent backdoor into e-commerce websites.The attack leverages CVE-2024-20720 (CVSS score: 9.1), which has been described by Adobe as a case of "improper neutralization of special elements" that could pave the way for arbitrary code execution.It was addressed by the company as part of

New Wave of JSOutProx Malware Targeting Financial Firms in APAC and MENA

The Hacker News - 05 April 2024 14:18

Financial organizations in the Asia-Pacific (APAC) and Middle East and North Africa (MENA) are being targeted by a new version of an "evolving threat" called JSOutProx."JSOutProx is a sophisticated attack framework utilizing both JavaScript and .NET," Resecurity said in a technical report published this week."It employs the .NET (de)serialization feature to interact with a core

Chinese Threat Actors Deploy New TTPs to Exploit Ivanti Vulnerabilities

Infosecurity Magazine - 05 April 2024 15:00

Scottish Cyber Coordination Centre

Mandiant research details how Chinese espionage groups are deploying new tools post-exploitation of recently patched Ivanti vulnerabilities