Scottish
Cyber
Coordination
Centre

# Daily threat bulletin

19 December 2024

## Vulnerabilities

### Threat actors are attempting to exploit Apache Struts vulnerability CVE-2024-53677

Security Affairs - 18 December 2024 21:20

Researchers warn that threat actors are attempting to exploit a recently disclosed Apache Struts vulnerability CVE-2024-53677. Researchers warn that threat actors are attempting to exploit the vulnerability CVE-2024-53677 (CVSS score of 9.5) in Apache Struts.

### BeyondTrust Issues Urgent Patch for Critical Vulnerability in PRA and RS Products

The Hacker News - 18 December 2024 15:45

BeyondTrust has disclosed details of a critical security flaw in Privileged Remote Access (PRA) and Remote Support (RS) products that could potentially lead to the execution of arbitrary commands.

### New Attacks Exploit VSCode Extensions and npm Packages

Infosecurity Magazine - 18 December 2024 15:00

Malicious campaigns targeting VSCode extensions have recently expanding to npm, risking software supply chains.

### CISA Adds Four Known Exploited Vulnerabilities to Catalog

CISA Advisories -

CISA has added four new vulnerabilities to its Known Exploited Vulnerabilities Catalog, based on evidence of active exploitation: CVE-2018-14933 NUUO NVRmini Devices OS Command Injection Vulnerability; CVE-2022-23227 NUUO NVRmini 2 Devices Missing Authentication Vulnerability; CVE-2019-11001 Reolink Multiple IP Cameras OS Command Injection Vulnerability; CVE-2021-40407 Reolink RLC-410W IP Camera OS Command Injection Vulnerability.

## Threat actors and malware

### Ongoing phishing attack abuses Google Calendar to bypass spam filters

BleepingComputer - 18 December 2024 19:16

An ongoing phishing scam is abusing Google Calendar invites and Google Drawings pages to steal credentials while bypassing spam filters. [...]

### HubPhish Abuses HubSpot Tools to Target 20,000 European Users for Credential Theft

The Hacker News - 18 December 2024 20:40

Cybersecurity researchers have disclosed a new phishing campaign that has targeted European companies with an aim to harvest account credentials and take control of the victims' Microsoft Azure cloud infrastructure.

### Attacker Distributes DarkGate Using MS Teams Vishing Technique

Infosecurity Magazine - 18 December 2024 13:15

Trend Micro highlighted a case where an attacker posed as a client on an MS Teams call to distribute DarkGate malware

### Russia-linked APT29 group used red team tools in rogue RDP attacks

Security Affairs - 18 December 2024 23:24

Russia-linked APT29 group uses malicious RDP configuration files, adapting red teaming methods for cyberattacks to compromise systems. In October 2024, the Russia-linked cyber espionage group APT29 used rogue RDP attacks via phishing emails targeting governments, think tanks, and Ukrainian entities to steal data and install malware.

### Hacker Leaks Cisco Data

SecurityWeek - 18 December 2024 10:27

IntelBroker has leaked 2.9 Gb of data stolen recently from a Cisco DevHub instance, but claims it's only a fraction of the total.