Scottish Cyber Coordination Centre

# Daily threat bulletin

15 October 2024

## Vulnerabilities

### Jetpack fixes critical information disclosure flaw existing since 2016

BleepingComputer - 14 October 2024 16:30

WordPress plugin Jetpack released a critical security update earlier today, addressing a vulnerability that allowed a logged-in user to access forms submitted by other visitors to the site. [...]

### Nation-state actor exploited three Ivanti CSA zero-days

Security Affairs - 14 October 2024 17:58

An alleged nation-state actor exploited three zero-day vulnerabilities in Ivanti Cloud Service Appliance (CSA) in recent attacks. Fortinet FortiGuard Labs researchers warn that a suspected nation-state actor has been exploiting three Ivanti Cloud Service Appliance (CSA) zero-day issues to carry out malicious activities.

### Thousands of Fortinet instances vulnerable to actively exploited flaw

The Register - 14 October 2024 13:30

No excuses for not patching this nine-month-old issue More than 86,000 Fortinet instances remain vulnerable to the critical flaw that attackers started exploiting last week, according to Shadowserver's data.

### Juniper Networks Patches Dozens of Vulnerabilities

SecurityWeek - 14 October 2024 12:04

Juniper Networks has announced patches for dozens of vulnerabilities in Junos OS, Junos OS Evolved, and third-party components.

## Threat actors and malware

### TrickMo malware steals Android PINs using fake lock screen

BleepingComputer - 14 October 2024 14:34

Forty new variants of the TrickMo Android banking trojan have been identified in the wild, linked to 16 droppers and 22 distinct command and control (C2) infrastructures, with new features designed to steal Android PINs. [...]

### Supply Chain Attacks Can Exploit Entry Points in Python, npm, and Open-Source Ecosystems

Scottish Cyber Coordination Centre

The Hacker News - 14 October 2024 17:38

Cybersecurity researchers have found that entry points could be abused across multiple programming ecosystems like PyPI, npm, Ruby Gems, NuGet, Dart Pub, and Rust Crates to stage software supply chain attacks.

## Imperva Defends Against Targeted Exploits Used By APT29 Hackers

Security Boulevard - 14 October 2024 18:45

Recently, U.S. and U.K. cyber agencies have warned of a renewed wave of attacks led by Russian APT29 hackers. These sophisticated threat actors have been actively exploiting vulnerabilities in Zimbra Collaboration Suite and JetBrains TeamCity, specifically CVE-2022-27924 and CVE-2023-42793, to target critical systems.

## CISA and FBI Release Fact Sheet on Protecting Against Iranian Targeting of Accounts Associated with National Political Organizations

CISA Advisories -

Today, CISA and the Federal Bureau of Investigation (FBI) released joint fact sheet, How to Protect Against Iranian Targeting of Accounts Associated with National Political Organizations. This fact sheet provides information about threat actors affiliated with the Iranian Government's Islamic Revolutionary Guard Corps (IRGC) targeting and compromising accounts of Americans to stoke discord and undermine confidence in U.S. democratic institutions.