Scottish Cyber Coordination Centre

Daily threat bulletin

29 July 2024

Vulnerabilities

Google fixes Chrome Password Manager bug that hides credentials

BleepingComputer - 26 July 2024 16:04

Google has fixed a bug in Chrome's Password Manager that caused user credentials to disappear temporarily for more than 18 hours.

BIND updates fix four high-severity DoS bugs in the DNS software suite

Security Affairs - 26 July 2024 12:07

The Internet Systems Consortium (ISC) released BIND security updates that fixed several remotely exploitable DoS bugs in the DNS software suite. The Internet Systems Consortium (ISC) released security updates for BIND that address DoS vulnerabilities that could be remotely exploited. An attacker can exploit these vulnerabilities to disrupt DNS services. ISC addressed four high-severity vulnerabilities.

Millions of Devices Vulnerable to 'PKFail' Secure Boot Bypass Issue

darkreading - 26 July 2024 22:08

Several vendors for consumer and enterprise PCs share a compromised crypto key that should never have been on the devices in the first place.

Progress Patches Critical Telerik Report Server Vulnerability

SecurityWeek - 26 July 2024 14:43

Progress Software calls attention to a critical remote code execution flaw in the Telerik Report Server product.

CISA Adds Two Known Exploited Vulnerabilities to Catalog

CISA Advisories -

CISA has added two new vulnerabilities to its Known Exploited Vulnerabilities Catalog, based on evidence of active exploitation - CVE-2012-4792 Microsoft Internet Explorer Use-After-Free Vulnerability; CVE-2024-39891 Twilio Authy Information Disclosure Vulnerability.

Threat actors and malware

Security Affairs Malware Newsletter – Round 4

Security Affairs - 28 July 2024 16:13

Scottish Cyber Coordination Centre

Security Affairs Malware newsletter includes a collection of the best articles and research on malware in the international landscape. Play Ransomware Group's New Linux Variant Targets ESXi, Shows Ties With Prolific Puma Fake Browser Updates Lead to BOINC Volunteer Computing Software.

Gh0st RAT Trojan Targets Chinese Windows Users via Fake Chrome Site

The Hacker News - 29 July 2024 11:26

The remote access trojan known as Gh0st RAT has been observed being delivered by an "evasive dropper" called Gh0stGambit as part of a drive-by download scheme targeting Chinese-speaking Windows users.

Malicious PyPI Package Targets macOS to Steal Google Cloud Credentials

The Hacker News - 27 July 2024 12:17

Cybersecurity researchers have discovered a malicious package on the Python Package Index (PyPI) repository that targets Apple macOS systems with the goal of stealing users' Google Cloud credentials from a narrow pool of victims. The package, named "lr-utils-lib," attracted a total of 59 downloads before it was taken down.

FBI, CISA, and Partners Release Advisory Highlighting North Korean Cyber Espionage Activity

CISA Advisories -

Today, CISA—in partnership with the Federal Bureau of Investigation (FBI)—released a joint Cybersecurity Advisory, North Korea State-Sponsored Cyber Group Conducts Global Espionage Campaign to Advance Regime's Military and Nuclear Programs.