WEEKLY BULLETIN

1-5 JANUARY 2024

Quote of the week

"Cybersecurity is not just a technology, but a mindset—where vigilance shields the digital realm, and resilience ensures a secure future in the ever-evolving landscape of the online world."

Content:

Nearly 11 million SSH servers vulnerable to new "Terrapin" attacks

Almost 11 million SSH (Secure Shell) servers exposed to the Internet are vulnerable to the Terrapin attack that threatens the integrity of some SSH connections.

The Terrapin attack targets the SSH protocol, affecting both clients and servers, and was developed by academic researchers from Ruhr University Bochum in Germany.

Read more

Data breach at healthcare technology firm affects 4.5 million patients

HealthEC LLC, a provider of health management solutions, suffered a data breach affecting nearly 4.5 million individuals.

HealthEC provides a population health management (PHM) platform that healthcare organizations can use for data integration, analytics, care coordination, patient engagement, compliance and reporting.

There are 17 health care service providers and state-level health systems that were affected by the cyber attack on HealthEC.

Read more

CISA warns of actively exploited vulnerabilities in Chrome and Excel

CISA has added two security vulnerabilities to its KEV catalog, a recently patched vulnerability in Google Chrome and a vulnerability affecting the open source library for reading information in an Excel file called Spreadsheet::ParseExcel.

America's Cyber Defense Agency has given federal agencies until January 23 to mitigate the two security issues identified as CVE-2023-7024 and CVE-2023-7101 according to the guidelines or stop using the vulnerable products.

Read more

PATCHING ALERT

ivanti

Ivanti- patching alert

IIvanti has discovered two actively exploited zero-day vulnerabilities that allow attackers to execute arbitrary commands on targeted ports.

The first security vulnerability (CVE-2023-46805) is an authentication bypass in the web component of the device, enabling attackers to access restricted resources by bypassing security controls, while the second (identified as CVE-2024-21887) is a vulnerability that allows authenticated administrators to execute arbitrary commands on vulnerable devices by sending specially crafted requests.

Read more

Rruga "Papa Gjon Pali II", No.3
info@cesk.gov.al

Autoriteti Kombëtar për CESK

autoriteti_kombetar_cesk

+35542221039