BRITISH COLUMBIA

****

Number: AL23-012
Date: August 3, 2023

Title

2022 Top routinely exploited vulnerabilities

Audience

This Alert is intended for IT professionals and managers of notified organizations.

Purpose

An Alert is used to raise awareness of a recently identified cyber threat that may impact cyber information assets, and to provide additional detection and mitigation advice to recipients. The Canadian Centre for Cyber Security ("Cyber Centre") is also available to provide additional assistance regarding the content of this Alert to recipients as requested.

Details

On August 1, 2023, the Canadian Centre for Cyber Security (CCCS) joined cyber security partners from the Cybersecurity and Infrastructure Security Agency (CISA), Federal Bureau of Investigation (FBI), National Security Agency (NSA), Australian Cyber Security Centre (ACSC), New Zealand Computer Emergency Response Team (CERT-NZ) and National Cyber Security Centre (NCSC-NZ) and the United Kingdom's National Cyber Security Centre (NCSC-UK) to publish a joint Cybersecurity Advisory (CSA) detailing the Common Vulnerabilities and Exposures (CVEs) routinely and frequently exploited by malicious cyber actors in 2022 and the associated Common Weakness Enumerations (CWEs) [1]

This joint advisory is being published to provide awareness on the CVEs routinely and frequently exploited by malicious cyber actors and the mitigations organizations can take to protect themselves. The Joint Cybersecurity Advisory highlights that in 2022, malicious cyber actors exploited more older software vulnerabilities than recently disclosed vulnerabilities to target unpatched, internet-facing systems. Malicious cyber actors generally have the most success exploiting these known, older, and globally prevalent vulnerabilities and will prioritize the development of exploits or use publicly available Proof of concept (PoC) code.

The Cybersecurity Advisory (CSA) contains a list of the most routinely exploited vulnerabilities, steps for vendors and developers to ensure their products are secure-by-design and default, and mitigations for end-user organizations to improve their cyber security posture. Additional guidance is available in the Cyber Centre's Top 10 IT security actions to protect Internet connected networks and information - ITSM.00.089 [2]. These publications are based on analysis of cyber threat trends to help minimize intrusions or the impacts of a successful cyber intrusion. The authoring organizations encourage timely patching to reduce the effectiveness of known exploits as well as hunting for malicious activity using guidance found in the referenced CSA to reduce the likelihood and impact of future incidents.

References

[1] 2022 Top Routinely Exploited Vulnerabilities - Joint Cybersecurity Advisory
[2] Top 10 IT security actions to protect Internet connected networks and information -ITSM.00.089

****