HC3: Alert

April 27, 2022 TLP: WHITE Report: 202204271200

2021 Top Routinely Exploited Vulnerabilities

Executive Summary

U.S., Australian, Canadian, New Zealand, and UK cybersecurity authorities assess, in 2021, malicious cyber actors aggressively targeted newly disclosed critical software vulnerabilities against broad target sets, including public and private sector organizations worldwide. To a lesser extent, malicious cyber actors continued to exploit publicly known, dated software vulnerabilities across a broad spectrum of targets. This advisory provides details on the top 15 Common Vulnerabilities and Exposures (CVEs) routinely exploited by malicious cyber actors in 2021, as well as other frequently exploited CVEs.

Report

AA22-117A - 2021 Top Routinely Exploited Vulnerabilities
https://www.cisa.gov/uscert/ncas/alerts/aa22-117a

Impact to HPH Sector

This list of routinely exploited vulnerabilities applies to all critical infrastructure sectors.

The cybersecurity authorities encourage organizations to apply the recommendations in the Mitigations section of this Cybersecurity Advisory, to include:

- Updating software, operating systems, applications, and firmware on IT network assets in a timely manner.
- Using a centralized patch management system.
- Replacing end-of-life software, i.e., software that is no longer supported by the vendor.
- Enforcing multifactor authentication (MFA) for all users, without exception.
- Properly configuring and securing internet-facing network devices, disabling unused or unnecessary network ports and protocols, encrypting network traffic, and disabling unused network services and devices.

All organizations should immediately report incidents to CISA at https://us-cert.cisa.gov/report, a local FBI Field Office, or U.S. Secret Service Field Office. CISA also offers a range of no-cost cyber hygiene services to help organizations assess, identify, and reduce their exposure to threats. By requesting these services, organizations of any size could find ways to reduce their risk and mitigate attack vectors.

References

Links to additional references and resources can be found in the above referenced report.

Contact Information

If you have any additional questions, please contact us at HC3@hhs.gov.

We want to know how satisfied you are with our products. Your answers will be anonymous, and we will use the responses to improve all our future updates, features, and new products. Share Your Feedback