HC3: Alert

October 1, 2021 TLP: White Report: 202110011400

Hardening Remote Access VPN Amplify Alert

Executive Summary

The NSA and CISA issued a joint information sheet providing guidance on hardening Virtual Private Networks (VPNs) services. VPNs are known to allow users to remotely connect to a corporate network and access internal materials via a secure tunnel. Because remote access VPN servers are entry points into protected networks, they are targets for adversaries. The NSA and CISA advises selecting standards-based VPNs from reputable vendors with a proven track record of quickly remediating vulnerabilities and following best practices in regard to using strong authentication credentials.

Report

Selecting and Hardening Remote Access VPN Solutions
https://media.defense.gov/2021/Sep/28/2002863184/-1/-1/0/CSI_SELECTING-HARDENING-REMOTE-ACCESS-VPNS-20210928.PDF

Impact to HPH Sector

The health sector is known to frequently use VPN technologies for telehealth, telemedicine, patient access to records and appointments as well as a variety of other applications. Compromise can lead to disruption of healthcare operations and leaking of sensitive health information, including research-related intellectual property as well as protected employee and patient information, leading to a leak of personal health information (PHI) and a potential HIPAA violation. HC3 recommends that healthcare organizations review the NSA/CISA join information sheet and take appropriate actions in accordance with their risk management strategy.

References

Guide to IPsec VPNs
https://csrc.nist.gov/publications/detail/sp/800-77/rev-1/final
Selecting and Hardening Remote Access VPN Solutions
https://media.defense.gov/2021/Sep/28/2002863184/-1/-1/0/CSI_SELECTING-HARDENING-REMOTE-ACCESS-VPNS-20210928.PDF
National Cyber Security Center, Cybersecurity and Infrastructure Security Agency, Federal Bureau of Investigation, and National Security Agency (2021), Advisory: Further TTPs associated with SVR cyber actors
https://www.ncsc.gov.uk/files/Advisory Further TTPs associated with SVR cyber actors.pdf

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