



**Newport News
Shipbuilding**

SUPPLIER SECURITY BULLETIN

Critical Vulnerability: Sophos Firewall

April 18, 2022

Newport News Shipbuilding (NNS) would like to make all Defense Industrial Base (DIB) suppliers and partners aware of a Remote Code Execution vulnerability with Sophos firewalls.

[CVE-2022-1040](#) is a critical vulnerability that is being actively exploited by external attackers. Due to its severity and ease of exploit, the Cybersecurity and Infrastructure Security Agency (CISA) has added this vulnerability to the [Known Exploited Vulnerabilities Catalog](#) as a must remediate. Sophos has [remediations and workarounds](#) available at www.sophos.com/en-us/security-advisories/sophos-sa-20220325-sfos-rce.

Newport News Shipbuilding encourages all DIB organizations to review CISA's [Binding Operation Directive 22-01 \(BOD 22-01\)](#) and the [Known Exploited Vulnerabilities Catalog](#) and apply any necessary mitigations to applicable products.

As a reminder, in the unfortunate event that your organization suffers a compromise of company information systems, you should follow the incident reporting requirements of the DFARS Clause 252.204-7012 should any network or system process, store or transmit Controlled Unclassified Information (CUI). Additionally, please report any compromise to NNS Security via Cyber@hii-co.com.

Thank you for your attention to this important matter.

Questions regarding this bulletin may be directed to your NNS Buyer or NNS Security.

A DIVISION OF HUNTINGTON INGALLS INDUSTRIES

4101 Washington Avenue • Newport News, VA 23607 • Telephone (757) 380-2000 • www.huntingtoningalls.com