

CSP Vulnerability Scanner™

It is a vulnerability scanning and reporting solution for HPE NonStop systems that analyzes risks and identifies vulnerabilities by checking the NonStop system's configuration, access permissions, and security settings. It generates insightful reports for users and recommends changes to improve the security posture.

To effectively audit the security of the systems, the CSP Vulnerability Scanner gathers a vast amount of information from different sources, including Safeguard, Guardian, and other subsystems. It automates this task by providing reports and analysis from a single source for both technical and non-technical users.

The CSP Vulnerability Scanner also includes access to CSP-Wiki®, where users can get more details on the settings, security, and compliance implications.



Installation & Use

The installation process is quick, and the solution is easy to use. There are two ways to select the desired scans & generate reports:

- VSREPORT Macro- This TACL macro guides the users to build a report
- TACL command line – For users that are very familiar with command syntax

The users will be able to select from a list of available reports and, based on the selection, may be prompted for some additional information.



Key Features

- Scans NonStop systems to identify vulnerabilities
- Provides recommendations to improve security
- Very easy to install and use
- Quickly perform scans and generate insightful reports
- Easily select from list of available reports
- Export reports with Spoolview
- Share reports with management and auditors

Types of Reports

- Security Analysis Report
- Authorization Report
- Examine Sub-volume Access Report
- Explain Access to Object Report
- Group Members Report
- Show Access Report
- Safeguard Globals Report