
SwiftEdge Security & Optimizer



Project Advisor: Dr. Sean Hayes
April 24th, 2026

Noah Huber & Daniel Howard
Cybersecurity Major
Charleston Southern University

Table Of Contents

- Modern Problems
- What is SwiftEdge Security & Optimizer
- Walkthrough & Demo
- Project Goals
- Testing
- Challenges
- Future Development
- Q/A

Modern Problems

01

Modern Problems

Windows systems become slower, less organized, and less secure over time.

The tools to fix those issues are time consuming and far spread. Identifying vulnerable software can be difficult.

SwiftEdge addresses this by bringing those core functions into one simple, lightweight application.

Problem

● Slower

Windows becomes much slower over time.

● Less Organized

Frequent use reduces file system organization.

● Insecure

As Windows OS ages, it becomes insecure or obsolete.

Opportunity

● Unique Tool

A tool that combines functionality of other tools.

● Lightweight Application

Many of the current applications or tools require large downloads or are resources intensive.

Solution

● SwiftEdge

SwiftEdge combines tools, scripts, and other software to craft an all-in-one lightweight utility for Windows, including vulnerability scanning.

SwiftEdge Security & Optimizer

5

Performance Tweaks | File Cleanup | Security Hardening | Vulnerability Scanning

Page

5

Welcome to SwiftEdge

SwiftEdge Security & Optimizer is a lightweight software application designed to enhance computer performance and security in a single, streamlined solution. The project aims to eliminate the need for multiple optimization and security tools by integrating system cleanup, performance tuning, and enhanced cybersecurity practices all into one intuitive platform.

Recommended: Create a System Restore Point before proceeding.

☒ Create a System Restore Point before continuing

Continue

02

Technologies

PowerShell 5.1+

Windows Forms GUI (PS Embedded)

Windows Registry

System Services (Control Panel, powercfg)

PS2EXE Compiler/Packaging

NVD NIST API CVE JSON CACHE

Project Goals

Improve System Performance

Automate System File Cleanup

Strengthen Windows Security

Scan for Software Vulnerabilities

Testing

Manual Testing

- SwiftEdge Security & Optimizer has built-in logging for module completion assurance.
- Test Cases, Logging, Module Functionality, & Completion were Tested in accordance to the test cases in our testing document.
- Tested with VM repeatability w/known vulnerabilities.

Testing (cont.)

Verification Metrics

Testing focused on module completion, measurable changes in execution time, registry changes, control panel settings, scanner output, and logging behavior.



Performance

Execution Time, Setting Changes, Logging, Completion.



Cleanup

Execution Time, Temporary File Cleanup, Log Dumps, Logging, Completion.



Security

Execution Time, Service Disablement, Registry Edits, Logging, Completion.



Scanning

CVE Matching/Execution Time, Application Scanning, Report Output, Caching, Logging, Completion.

SwiftEdge Security & Optimizer

Performance Tweaks | File Cleanup | Security Hardening | Vulnerability Scanning

Performance Cleanup Security **Vulnerability**

Vulnerability Module

Run the vulnerability scanner. Results will appear below:

```
Local JSON older than 1 day. Refreshing.
Downloading NVD feed: https://nvd.nist.gov/feeds/json/cve/2.0/nvdcve-2.0-2026.json.gz
Download complete. Extracting...
Extracted JSON to C:\Users\Noah Huber\AppData\Local\SwiftEdge\NVD\nvdcve-2026.json
Loading CVE JSON...
Loaded 9790 CVEs for 2026
Found 41 installed apps.
Scanning CVEs against installed apps...
=====
TOP 5 MOST VULNERABLE APPS
=====
Ranked by: severity rank CVSS score

Wireshark 4.2.2 arm64 (Version: 4.2.2)
Highest Severity: MEDIUM Rank: 2 Score: 5.3
Top CVEs:
- CVE-2026-0962 [MEDIUM 5.3]
=====
Recommended Actions
=====
- Use the official updater or vendor website for each listed application.
- If an app is unused, consider uninstalling it to reduce attack surface.
- After applying updates, rerun this scanner to confirm the vulnerabilities are reduced.
```

Run Vulnerability Scan

Challenges

03



Challenges

C.1 Vulnerability Scanning & NVD Rate Limits

- NVD API Rate Limits 5/30 Sec
- Live API queries limited
- Resorted to Yearly Cached JSON
- How to parse through 100K lines of the API.

C.2 PowerShell & Windows Forms

- Learning the intricacies of PowerShell & Windows Forms
- Major inspiration from ChrisTitus WinUtil
- Building an entire UI using Forms

C.3 Packaging w/PS2EXE

- Utilizing PS2EXE to compile and package an executable from multiple PowerShell scripts.
- Embedding multiple scripts at compilation does not behave like a normal compiler.
- Resorted to a single build script which creates a single PowerShell script & executable.

Future Development

04



Future Development

STIG Profiles

Add government-backed hardening options for stronger security.
Provide Additional Controls for Power Users.

Better Logging & Richer Scanner Output

Improve traceability of actions, errors, and verification of results.
Add richer scanner output for scanner runs and report results.
Major development could include automatically updating **Vulnerable Apps**.

Digital Certificate/ App Signing

Get digital certificate signing -> SwiftEdge is not flagged by Smartscreen or Defender.
Improved executable/application distribution & packaging.

Q & A

Any Questions, Comments, Concerns?

SwiftEdge Security & Optimizer

Performance Tweaks | File Cleanup | Security H

Performance Cleanup Security Vulnerability

Performance Module

Select which performance tweaks to apply:

- ☐ Ultimate Performance Power Plan
- ☐ Disable SysMain
- ☐ Disable Windows Search
- ☐ Disable DiagTrack
- ☐ Disable Window Animations
- ☐ Disable Transparency
- ☐ Disable Windows Tips
- ☐ Disable Hibernation
- ☐ Optimize Startup Delay
- ☐ Disable Startup Applications
- ☐ Enable Game Mode
- ☐ Enable Hardware-Acceleration

Reset Performance to Defaults

Run Selected Performance Tweaks

SwiftEdge Security
& Optimizer