SYNOPSYS®

Polaris Developer Detail SCA Report

Prepared on: **Jun 13, 2024 8:27 PM (GMT)**

Table of Contents

1. Introduction

Modern secure development practices focus on minimizing security risks in an application. The Synopsys® Polaris Software Integrity Platform™ provides an aggregated view of the application risk reported by various Synopsys security analysis tools and normalizes testing results to assess the overall security posture of applications under development.

1.1 Objective

This report presents the results of an application security analysis performed by the Polaris Software Integrity Platform™. This analysis identifies vulnerable areas in the different components of your application that may be exploited by a malicious user, and estimates the application's protection from common attacks. This report also assesses the overall security risk for your application across all threat areas.

1.2 Scope

The scope of this report is limited to components specific to the applications and projects listed:

Application	Project
Third-party GitHub Actions	setup-msbuild

2. Executive Summary

CISOs and security executives need to understand and manage their organization's security posture across their application portfolio. They need to identify, prioritize, and resolve critical security vulnerabilities that threaten their organizations. The Polaris Software Integrity Platform™ addresses these needs by combining the best-of-breed security tools with robust security reporting dashboards to provide cross-tool reporting focused on aggregation, normalization, and correlation.

3. Methodology

The Polaris Software Integrity Platform™ brings the power of Synopsys software integrity tools together into an integrated, easy-to-use solution that enables security and development teams to build secure, high-quality software faster. The specialized Application Security Testing (AST) tools on the Polaris Software Integrity Platform™, each covering specific aspects of the code base, deliver holistic application security coverage when used together.

This report was generated with the following configuration:

- Report created by: michael.henderson@keyfactor.com
- Severities Included: critical, high

4. Application Overview

4.1 Third-party GitHub Actions

C Critical	H High	Total
3	25	28

4.1.1 setup-msbuild

Project Name: setup-msbuild
Last Test Date: Thursday, June 6, 2024 11:30 PM

C Critical	H High	Total
3	25	28

ISSUE DETAILS

Component: tar 4.4.8

Origin External ID	Package URL	Short Term	Long Term
tar/4.4.8	pkg:npm/tar@4.4.8	4.4.19	6.1.15

Severity	Vulnerability ID	Issue Type	CWE	First Detected
High	CVE-2021-37712	Directory Traversal	CWE-22	May 30, 2024 11:31 PM
High	CVE-2021-32804	Weak Input Validation	CWE-20	May 30, 2024 11:31 PM
High	CVE-2021-32803	Weak Input Validation	CWE-20	May 30, 2024 11:31 PM
High	CVE-2021-37701	Directory Traversal	CWE-22	May 30, 2024 11:31 PM
High	CVE-2021-37713	Directory Traversal	CWE-22	May 30, 2024 11:31 PM

Component: ajv 6.10.2

Origin External ID	Package URL	Short Term	Long Term
ajv/6.10.2	pkg:npm/ajv@6.10.2	6.12.6	8.12.0

Severity	Vulnerability ID	Issue Type	CWE	First Detected
High	CVE-2020-15366	External Control of Critical State Data	CWE-642	May 30, 2024 11:31 PM
High	CVE-2020-15366	Modification of Assumed-Immutable Data (MAID)	CWE-471	May 30, 2024 11:31 PM
High	CVE-2020-15366	Mass Assignment	CWE-915	May 30, 2024 11:31 PM

Component: babel-traverse 7.7.4

Origin External ID	Package URL	Short Term	Long Term
@babel/traverse/7.7.4	pkg:npm/%40babel/traverse@7.7.4	7.22.10	7.22.10

Severity	Vulnerability ID	Issue Type	CWE	First Detected
High	CVE-2023-45133	Weak Input Validation	CWE-20	May 30, 2024 11:31 PM
High	CVE-2023-45133	Incomplete List of Disallowed Inputs	CWE-184	May 30, 2024 11:31 PM

Component: minimist 1.2.5

Origin External ID	Package URL	Short Term	Long Term
minimist/1.2.5	pkg:npm/minimist@1.2.5	1.2.8	1.2.8

Severity	Vulnerability ID	Issue Type	CWE	First Detected
High	BDSA-2020-4373	Weak Input Validation	CWE-20	May 30, 2024 11:31 PM
High	CVE-2021-44906	Modification of Assumed-Immutable Data (MAID)	CWE-471	May 30, 2024 11:31 PM

Component: fsevents 1.2.9

Origin External ID	Package URL	Short Term	Long Term
fsevents/1.2.9	pkg:npm/fsevents@1.2.9	1.2.13	2.3.2

Severity	Vulnerability ID	Issue Type	CWE	First Detected
High	CVE-2023-45311	Use of Hard-coded, Security-relevant Constants	CWE-547	May 30, 2024 11:31 PM
High	CVE-2023-45311	Embedded Malicious Code	CWE-506	May 30, 2024 11:31 PM

Component: minimist 0.0.8

Origin External ID	Package URL	Short Term	Long Term
minimist/0.0.8	pkg:npm/minimist@0.0.8	0.2.4	1.2.8

Severity	Vulnerability ID	Issue Type	CWE	First Detected
High	CVE-2021-44906	Modification of Assumed-Immutable Data (MAID)	CWE-471	May 30, 2024 11:31 PM
High	CVE-2020-7598	Weak Input Validation	CWE-20	May 30, 2024 11:31 PM

Component: minimist 1.2.0

Origin External ID	Package URL	Short Term	Long Term
minimist/1.2.0	pkg:npm/minimist@1.2.0	1.2.8	1.2.8

Severity	Vulnerability ID	Issue Type	CWE	First Detected
High	CVE-2021-44906	Modification of Assumed-Immutable Data (MAID)	CWE-471	May 30, 2024 11:31 PM

Severity	Vulnerability ID	Issue Type	CWE	First Detected
High	CVE-2020-7598	Weak Input Validation	CWE-20	May 30, 2024 11:31 PM

Component: yargs-parser 10.1.0

Origin External ID	Package URL	Short Term	Long Term
yargs-parser/10.1.0	pkg:npm/yargs-parser@10.1.0		21.1.1

Severity	Vulnerability ID	Issue Type	CWE	First Detected
Critical	CVE-2020-7608	Weak Input Validation	CWE-20	May 30, 2024 11:31 PM

Component: yargs-parser v13.1.1

Origin External ID	Package URL	Short Term	Long Term
yargs-parser/13.1.1	pkg:npm/yargs-parser@13.1.1	13.1.2	21.1.1

Severity	Vulnerability ID	Issue Type	CWE	First Detected
Critical	CVE-2020-7608	Weak Input Validation	CWE-20	May 30, 2024 11:31 PM

Component: npm ini 1.3.5

Origin External ID	Package URL	Short Term	Long Term
ini/1.3.5	pkg:npm/ini@1.3.5	1.3.8	4.1.1

Severity	Vulnerability ID	Issue Type	CWE	First Detected
High	CVE-2020-7788	Weak Input Validation	CWE-20	May 30, 2024 11:31 PM

Component: tough-cookie v2.5.0

Origin External ID	Package URL	Short Term	Long Term
tough-cookie/2.5.0	pkg:npm/tough-cookie@2.5.0		4.1.3

Severity	Vulnerability ID	Issue Type	CWE	First Detected
High	CVE-2023-26136	Mass Assignment	CWE-915	May 30, 2024 11:31 PM

Component: tough-cookie 2.4.3

Origin External ID	Package URL	Short Term	Long Term
tough-cookie/2.4.3	pkg:npm/tough-cookie@2.4.3	v2.5.0	4.1.2

Severity	Vulnerability ID	Issue Type	CWE	First Detected
High	CVE-2023-26136	Mass Assignment	CWE-915	May 30, 2024 11:31 PM

Component: node-fetch 2.1.2

Origin External ID	Package URL	Short Term	Long Term
node-fetch/2.1.2	pkg:npm/node-fetch@2.1.2	2.7.0	3.3.2

Severity	Vulnerability ID	Issue Type	CWE	First Detected
Critical	CVE-2022-0235	Open URL Redirect	CWE-601	May 30, 2024 11:31 PM

Component: jonschlinkert/unset-value 1.0.0

Origin External ID	Package URL	Short Term	Long Term
unset-value/1.0.0	pkg:npm/unset-value@1.0.0		2.0.1

Severity	Vulnerability ID	Issue Type	CWE	First Detected
High	BDSA-2021-4507	Mass Assignment	CWE-915	May 30, 2024 11:31 PM

Component: micromatch/braces 2.3.2

Origin External ID	Package URL	Short Term	Long Term
braces/2.3.2	pkg:npm/braces@2.3.2		3.0.2

Severity	Vulnerability ID	Issue Type	CWE	First Detected
High	BDSA-2024-2474	Uncontrolled Resource Consumption	CWE-400	May 30, 2024 11:31 PM

Component: json-schema 0.2.3

Origin External ID	Package URL	Short Term	Long Term
json-schema/0.2.3	pkg:npm/json-schema@0.2.3	0.4.0	0.4.0

Severity	Vulnerability ID	Issue Type	CWE	First Detected
High	CVE-2021-3918	Weak Input Validation	CWE-20	May 30, 2024 11:31 PM

Component: mikaelbr/node-notifier v5.4.3

Origin External ID	Package URL	Short Term	Long Term
node-notifier/5.4.3	pkg:npm/node-notifier@5.4.3	v5.4.5	10.0.1

Severity	Vulnerability ID	Issue Type	CWE	First Detected
High	CVE-2020-7789	Improper Neutralization of Special Elements used in a Command	CWE-77	May 30, 2024 11:31 PM

Component: is-typed-array 1.0.0

Origin External ID	Package URL	Short Term	Long Term
is-typedarray/1.0.0	pkg:npm/is-typedarray@1.0.0		