REVERSINGLABS

A Step-by-Step Walk Through of the ReversingLabs Software Assurance Service

How Software Development & Release Assess Security Readiness to Stop Supply Chain Risks

Erik Thoen

VP of Product Management, ReversingLabs

Thursday, October 28th, 1 PM ET

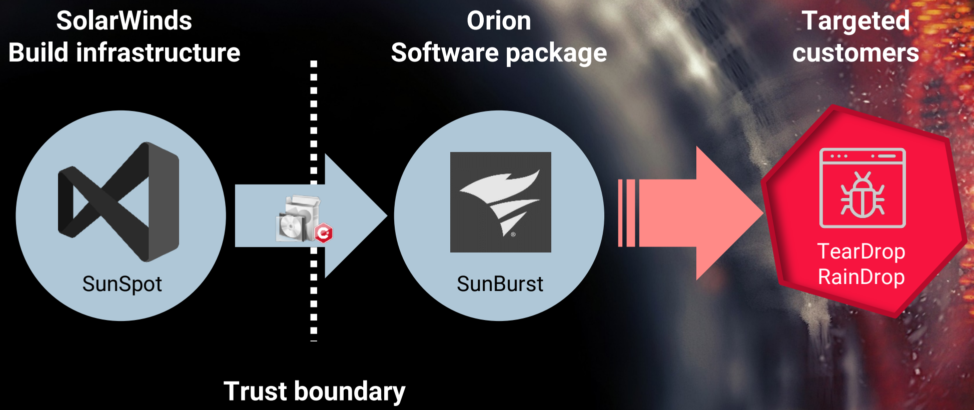
- Session will be recorded and will be sent to all registrants
- Please participate in poll questions throughout and survey at the end
- Questions will be answered at the end of the presentation

Agenda

- Supply chain attacks
- ReversingLabs approach
- Publisher and buyer workflows
- Demonstrations
- Deployment evolution
- Questions

SUNBURST

Attackers injected high quality rogue code through a build process compromise



DEFENDER'S PROBLEM

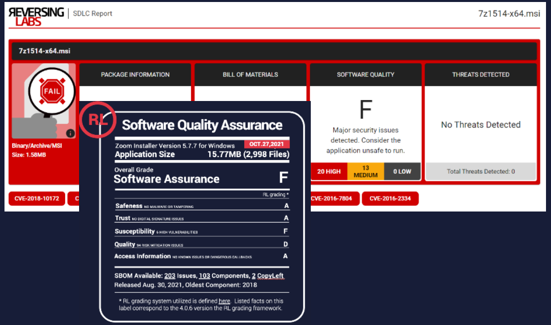
Not exploiting known vulnerabilities

Not known malware

Not poorly written code

Not using open-source libraries or code

Software Assurance Process Needed



SDLC Report 7z1514-x64.msi

7z1514-x64.msi

FAIL

Binary/Archive/MSI
Size: 1.58MB

PACKAGE INFORMATION | BILL OF MATERIALS | SOFTWARE QUALITY | THREATS DETECTED

F

Major security issues detected. Consider the application unsafe to run.

20 HIGH | 13 MEDIUM | 0 LOW

No Threats Detected

Total Threats Detected: 0

CVE-2018-10172 | CVE-2016-7804 | CVE-2016-2334

Software Quality Assurance

Zoom Installer Version 5.7.7 for Windows OCT.27,2021
Application Size 15.77MB (2,998 Files)

Overall Grade
Software Assurance F

RL grading *

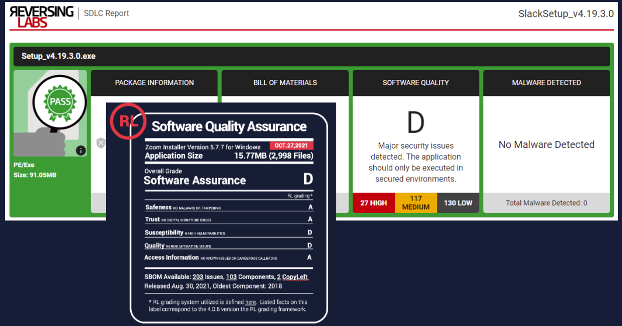
Safeness NO MALWARE OR TAMPERING	A
Trust NO DIGITAL SIGNATURE ISSUES	A
Susceptibility 6 HIGH VULNERABILITIES	F
Quality 94 RISK MITIGATION ISSUES	D
Access Information NO KNOWN ISSUES OR DANGEROUS CALLBACKS	A

SBOM Available: 203 Issues, 103 Components, 2 CopyLeft
Released Aug. 30, 2021, Oldest Component: 2018

* RL grading system utilized is defined here. Listed facts on this label correspond to the 4.0.6 version the RL grading framework.

SOFTWARE PRODUCERS

CODE IMPROVEMENT



SDLC Report SlackSetup_v4.19.3.0

Setup_v4.19.3.0.exe

PASS

PE/Exe
Size: 91.05MB

PACKAGE INFORMATION | BILL OF MATERIALS | SOFTWARE QUALITY | MALWARE DETECTED

D

Major security issues detected. The application should only be executed in secured environments.

27 HIGH | 117 MEDIUM | 130 LOW

No Malware Detected

Total Malware Detected: 0

Software Quality Assurance

Zoom Installer Version 5.7.7 for Windows OCT.27,2021
Application Size 15.77MB (2,998 Files)

Overall Grade
Software Assurance D

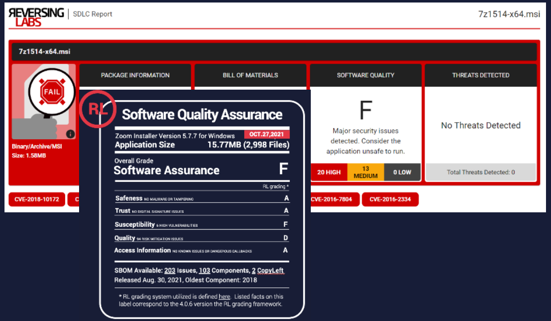
RL grading *

Safeness NO MALWARE OR TAMPERING	A
Trust NO DIGITAL SIGNATURE ISSUES	A
Susceptibility 6 HIGH VULNERABILITIES	D
Quality 94 RISK MITIGATION ISSUES	D
Access Information NO KNOWN ISSUES OR DANGEROUS CALLBACKS	A

SBOM Available: 203 Issues, 103 Components, 2 CopyLeft
Released Aug. 30, 2021, Oldest Component: 2018

* RL grading system utilized is defined here. Listed facts on this label correspond to the 4.0.6 version the RL grading framework.

✓



SDLC Report 7z1514-x64.msi

7z1514-x64.msi

FAIL

Binary/Archive/MSI
Size: 1.58MB

PACKAGE INFORMATION | BILL OF MATERIALS | SOFTWARE QUALITY | THREATS DETECTED

F

Major security issues detected. Consider the application unsafe to run.

20 HIGH | 13 MEDIUM | 0 LOW

No Threats Detected

Total Threats Detected: 0

CVE-2018-10172 | CVE-2016-7804 | CVE-2016-2334

Software Quality Assurance

Zoom Installer Version 5.7.7 for Windows OCT.27,2021
Application Size 15.77MB (2,998 Files)

Overall Grade
Software Assurance F

RL grading *

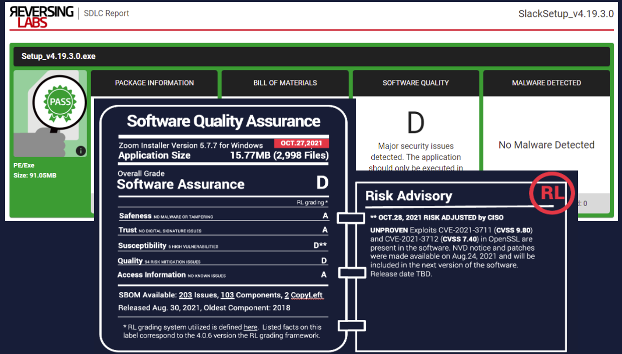
Safeness NO MALWARE OR TAMPERING A
Trust NO DIGITAL SIGNATURE ISSUES A
Susceptibility 6 HIGH VULNERABILITIES F
Quality 94 RISK MITIGATION ISSUES D
Access Information NO KNOWN ISSUES OR DANGEROUS CALLBACKS A

SBOM Available: 203 Issues, 103 Components, 2 CopyLeft
Released Aug. 30, 2021, Oldest Component: 2018

* RL grading system utilized is defined here. Listed facts on this label correspond to the 4.0.6 version the RL grading framework.

SOFTWARE BUYERS

RISK ASSESSMENT



SDLC Report SlackSetup_v4.19.3.0

Setup_v4.19.3.0.exe

PASS

PE/Exe
Size: 91.05MB

PACKAGE INFORMATION | BILL OF MATERIALS | SOFTWARE QUALITY | MALWARE DETECTED

D

Major security issues detected. The application should only be executed in

No Malware Detected

Software Quality Assurance

Zoom Installer Version 5.7.7 for Windows OCT.27,2021
Application Size 15.77MB (2,998 Files)

Overall Grade
Software Assurance D

RL grading *

Safeness NO MALWARE OR TAMPERING	A
Trust NO DIGITAL SIGNATURE ISSUES	A
Susceptibility 6 HIGH VULNERABILITIES	D**
Quality 94 RISK MITIGATION ISSUES	D
Access Information NO KNOWN ISSUES	A

SBOM Available: 203 Issues, 103 Components, 2 CopyLeft
Released Aug. 30, 2021, Oldest Component: 2018

* RL grading system utilized is defined here. Listed facts on this label correspond to the 4.0.6 version the RL grading framework.

Risk Advisory

**** OCT.28, 2021 RISK ADJUSTED by CISO**

UNPROVEN Exploits CVE-2021-3711 (**CVSS 9.80**) and CVE-2021-3712 (**CVSS 7.40**) in OpenSSL are present in the software. NVD notice and patches were made available on Aug.24, 2021 and will be included in the next version of the software. Release date TBD.

✓

Approach

Defending the next supply chain attack

DESIRED STATE

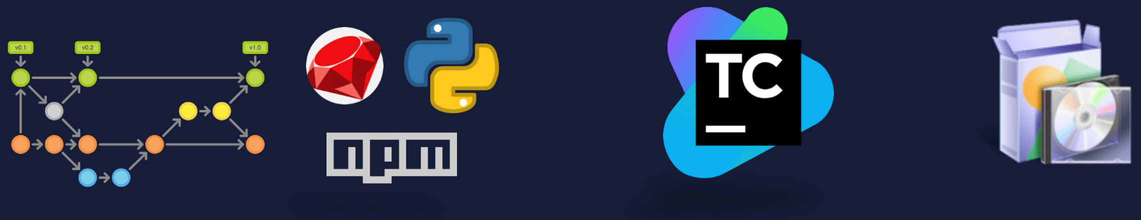
Defense requires a new analysis process

- Decomposing “golden” software image
- Describing underlying software behaviors
- Determining software deployment risks:

- Unknown behaviors ✓
- Known vulnerabilities ✓
- Enabled mitigations ✓
- Certificate validation ✓
- Sensitive information ✓
- Third party components ✓
- Embedded malware ✓

Publisher Workflow

Reduced supply chain risk



ReversingLabs

ReversingLabs

Source Control

Software Dependencies

Build Process

Release Image

Analyze software dependences before supply chain insertion

Release candidate software scan

AUTOMATED CHECKS

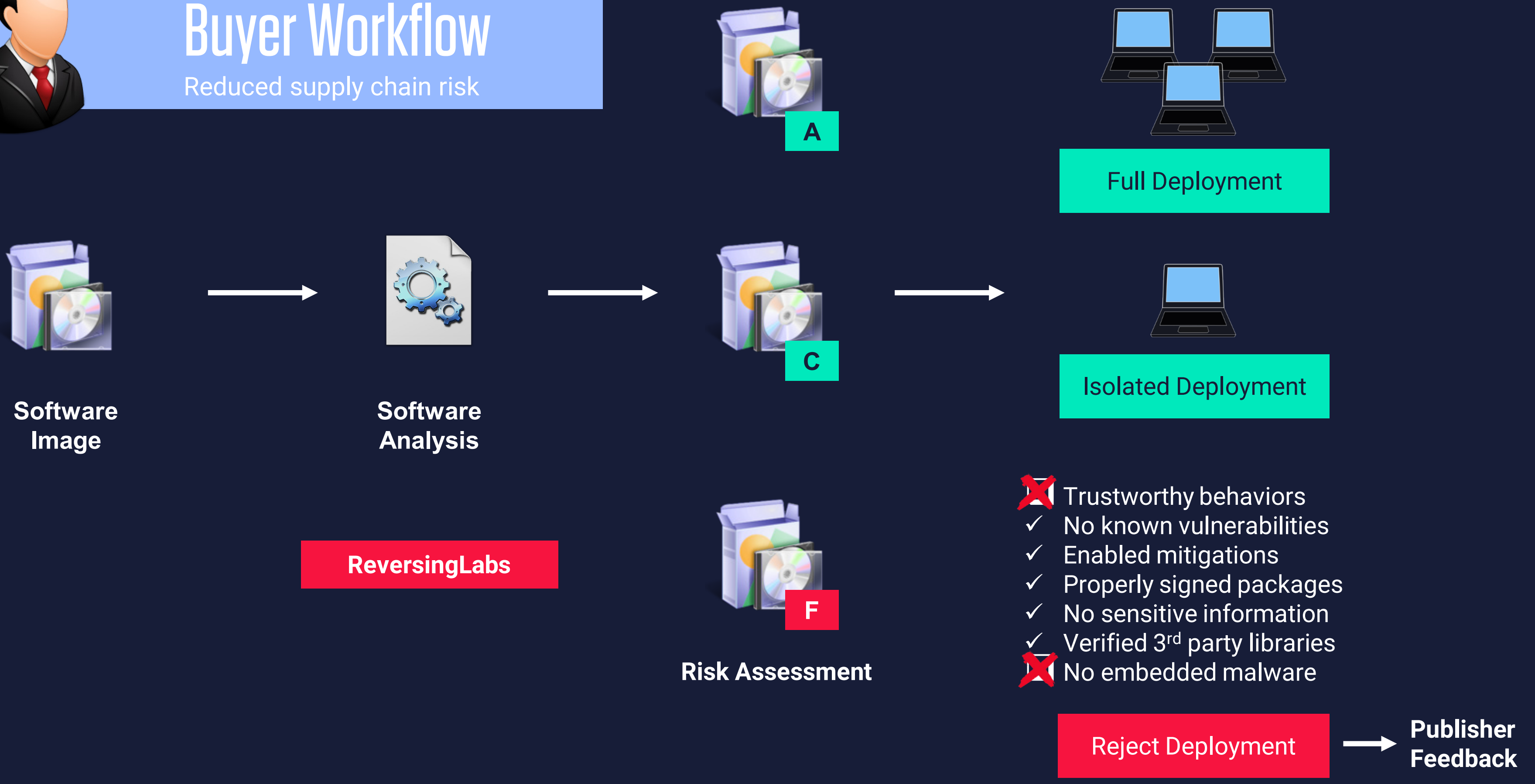
- ✓ No unknown behaviors
- ✓ No known vulnerabilities
- ✓ Enabled mitigations
- ✓ Properly signed packages
- ✓ No sensitive information
- ✓ Verified 3rd party libraries
- ✓ No embedded malware

RELEASE

REVERSINGLABS

Buyer Workflow

Reduced supply chain risk



Software Image

Software Analysis

ReversingLabs

A

C

F

Risk Assessment

Full Deployment

Isolated Deployment

- ☒ Trustworthy behaviors
- ✓ No known vulnerabilities
- ✓ Enabled mitigations
- ✓ Properly signed packages
- ✓ No sensitive information
- ✓ Verified 3rd party libraries
- ☒ No embedded malware

Reject Deployment → Publisher Feedback

REVERSINGLABS

Best Practices

New Capabilities for Compliance

WH.GOV

Executive Order on Improving the Nation's Cybersecurity

MAY 12, 2021 • PRESIDENTIAL ACTIONS

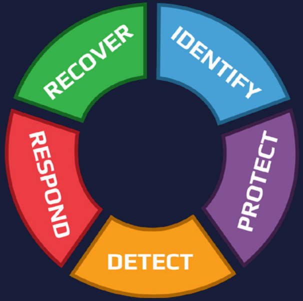
- Software Bill of Materials (SBOM)
- Component provenance
- Known and potential vulnerabilities

REVERSINGLABS carahsoft.

https://www.carahsoft.com/reversinglabs#contracts

NIST

Cybersecurity Framework



ReversingLabs Support

Identify:
- Asset Management
- Risk Assessment
- Supply Chain Risk Management

Protect:
- Data Security

Whitepaper: How ReversingLabs capabilities map to NIST CSF

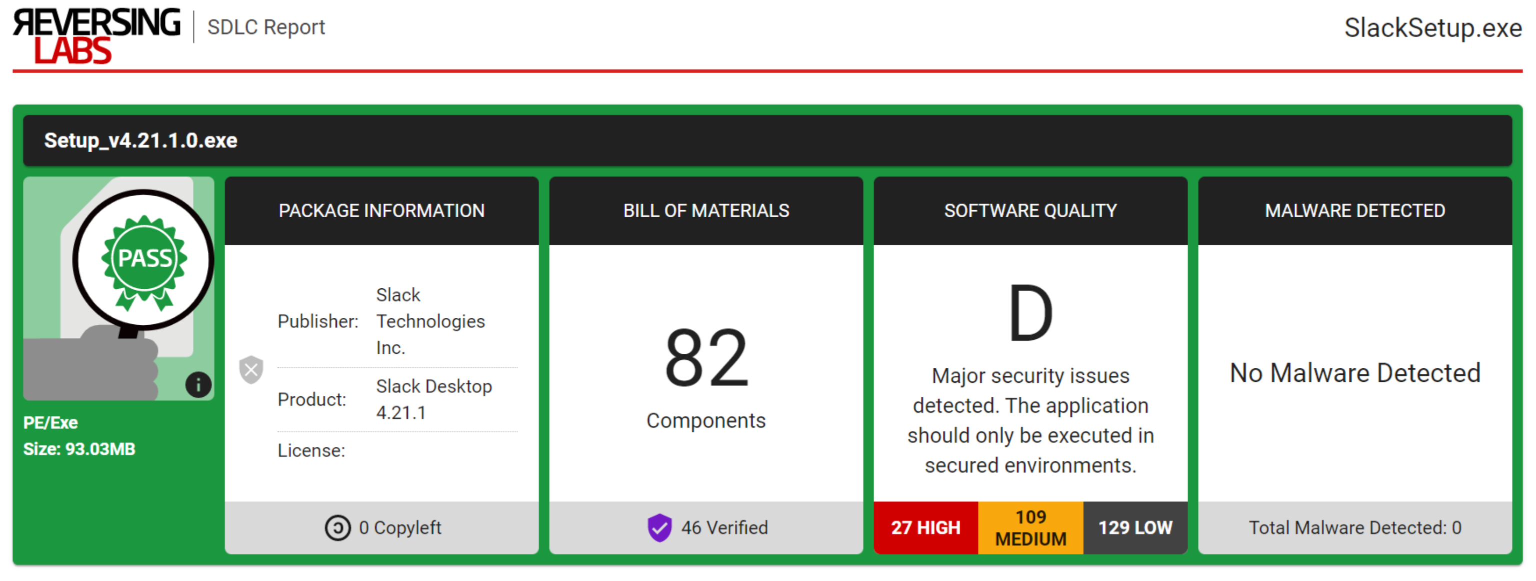
Poll Question #1:

What is your primary reason for researching an Application Security solution?

- We were breached
- Staying current given public attacks
- Executive directive to improve supply chain security and resiliency
- Existing AppSec tools not sufficient to verify software builds

Demo - Verified components

SlackSetup_v4.21.1.0



SDLC Report

SlackSetup.exe

Setup_v4.21.1.0.exe

PE/Exe
Size: 93.03MB

PACKAGE INFORMATION

Publisher:	Slack Technologies Inc.
Product:	Slack Desktop 4.21.1
License:	

0 Copyleft

BILL OF MATERIALS

82

Components

46 Verified

SOFTWARE QUALITY

D

Major security issues detected. The application should only be executed in secured environments.

27 HIGH	109 MEDIUM	129 LOW

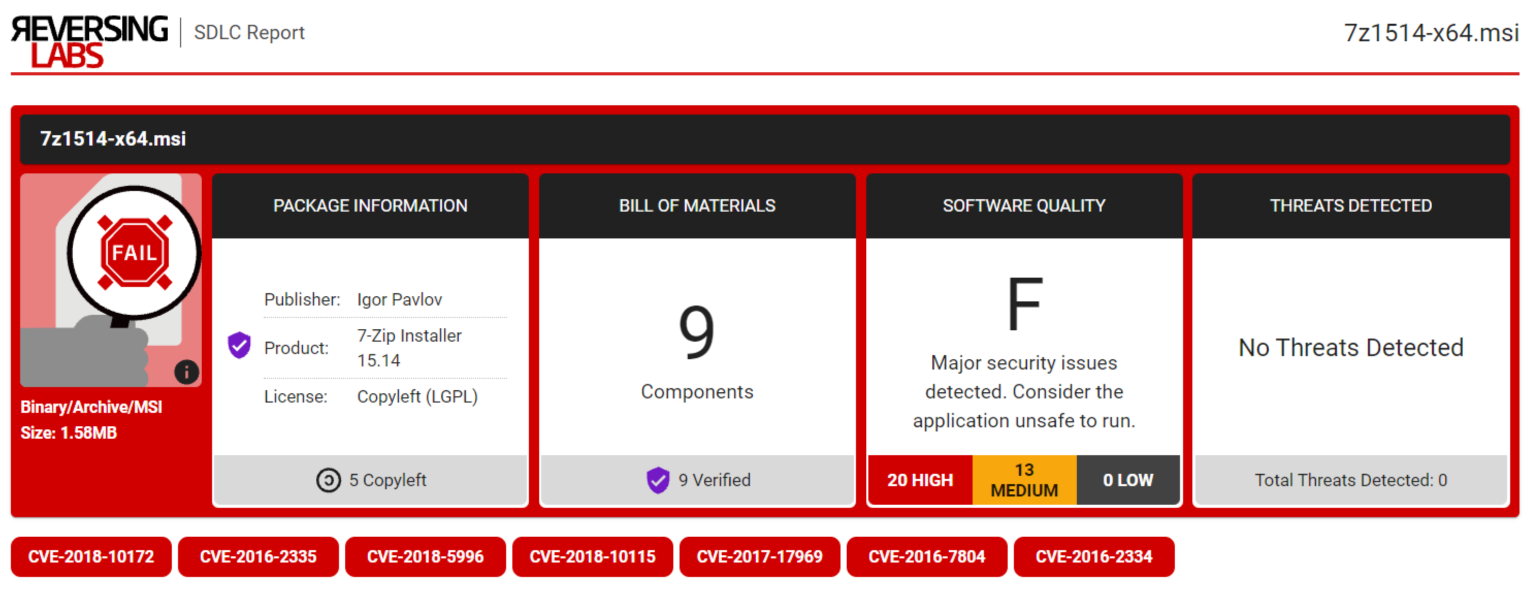
MALWARE DETECTED

No Malware Detected

Total Malware Detected: 0

Demo - Mitigated vulnerabilities

7z1514-x64.msi



SDLC Report

7z1514-x64.msi

7z1514-x64.msi

Binary/Archive/MSI
Size: 1.58MB

PACKAGE INFORMATION	BILL OF MATERIALS	SOFTWARE QUALITY	THREATS DETECTED
Publisher: Igor Pavlov Product: 7-Zip Installer 15.14 License: Copyleft (LGPL)	9 Components	F Major security issues detected. Consider the application unsafe to run.	No Threats Detected
5 Copyleft	9 Verified	20 HIGH · 13 MEDIUM · 0 LOW	Total Threats Detected: 0

CVE-2018-10172 CVE-2016-2335 CVE-2018-5996 CVE-2018-10115 CVE-2017-17969 CVE-2016-7804 CVE-2016-2334

REVERSINGLABS

Poll Question #2:

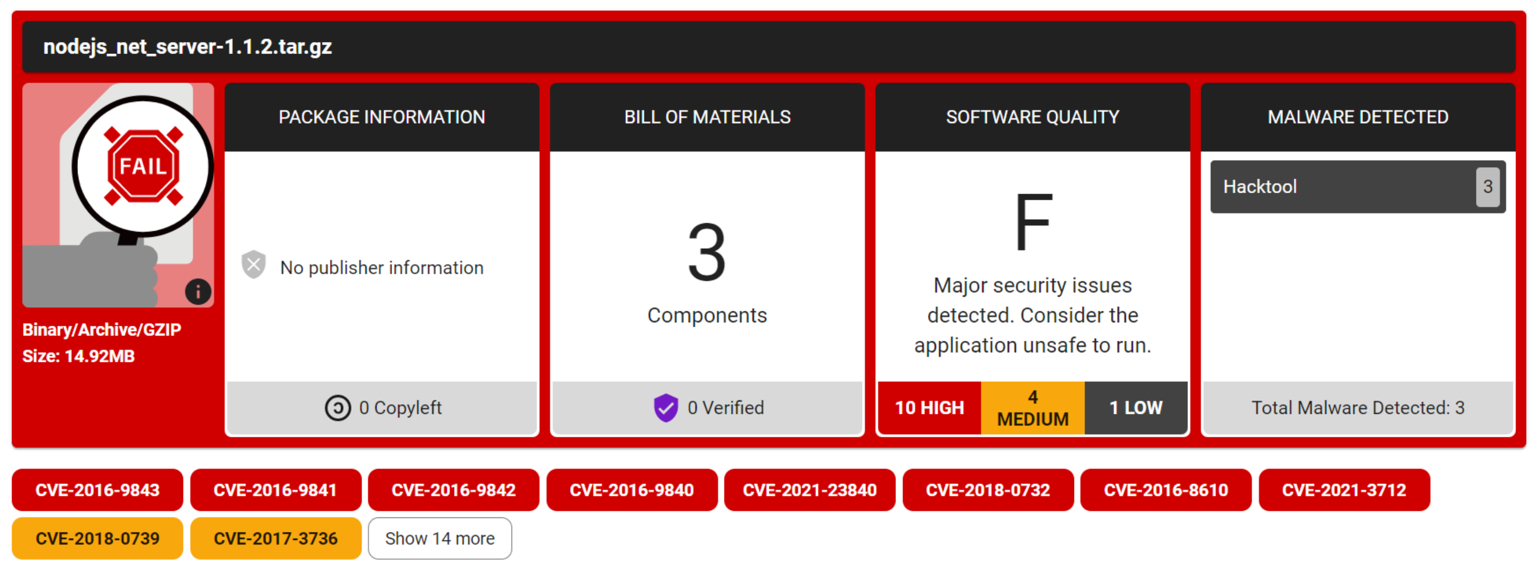
What are your top software supply chain security issues?

- Software tampering (hidden malware, compromised libraries, unsigned software, misconfigured code)
- Code quality and vulnerable software
- Open-source risks (npm, GitHub, etc.)
- 3rd Party COTS verification

REVERSINGLABS

Demo - Trustworthy behaviors

nodejs_net_server-1.1.2.tar.gz



nodejs_net_server-1.1.2.tar.gz

Binary/Archive/GZIP
Size: 14.92MB

PACKAGE INFORMATION

No publisher information

0 Copyleft

BILL OF MATERIALS

3
Components

0 Verified

SOFTWARE QUALITY

F
Major security issues detected. Consider the application unsafe to run.

10 HIGH | 4 MEDIUM | 1 LOW

MALWARE DETECTED

Hacktool 3

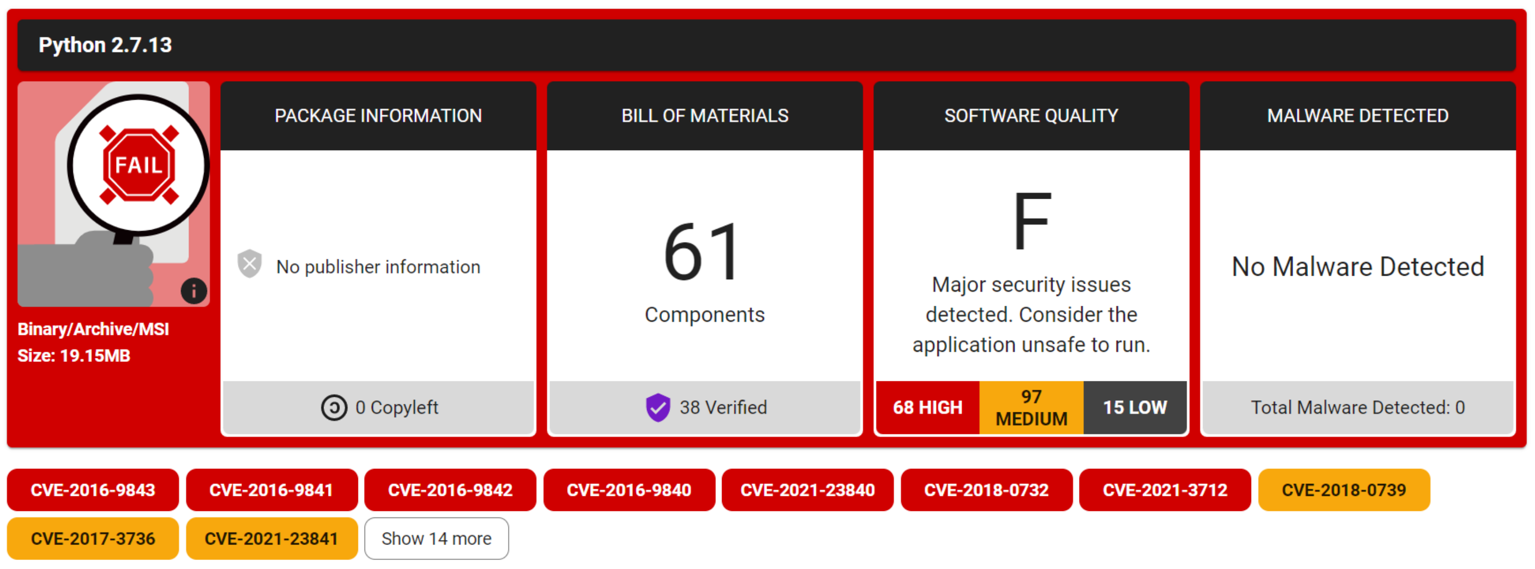
Total Malware Detected: 3

CVE-2016-9843 CVE-2016-9841 CVE-2016-9842 CVE-2016-9840 CVE-2021-23840 CVE-2018-0732 CVE-2016-8610 CVE-2021-3712

CVE-2018-0739 CVE-2017-3736 Show 14 more

Demo - Protected secrets

python-2.7.13.amd64.msi



Python 2.7.13

Binary/Archive/MSI
Size: 19.15MB

PACKAGE INFORMATION	BILL OF MATERIALS	SOFTWARE QUALITY	MALWARE DETECTED
No publisher information	61 Components	F Major security issues detected. Consider the application unsafe to run.	No Malware Detected
0 Copyleft	✓ 38 Verified	68 HIGH · 97 MEDIUM · 15 LOW	Total Malware Detected: 0

CVE-2016-9843 CVE-2016-9841 CVE-2016-9842 CVE-2016-9840 CVE-2021-23840 CVE-2018-0732 CVE-2021-3712 CVE-2018-0739
CVE-2017-3736 CVE-2021-23841 Show 14 more

Publisher Deployment Evolution

Phased Implementation

Software Assurance Managed Service

Initial Package Analysis

- ✓ Analyze key packages
- ✓ Provide reports
- ✓ Review and prioritize issues
- ✓ Evaluate component risks
- ✓ Discuss mitigation strategies
- ✓ Discuss development feedback

Differential Package Analysis

- ✓ Analyze new versions
- ✓ Provide differential reports
- ✓ Identify high-risk changes
- ✓ Evaluate component changes
- ✓ Modify mitigations strategies
- ✓ Modify development feedback

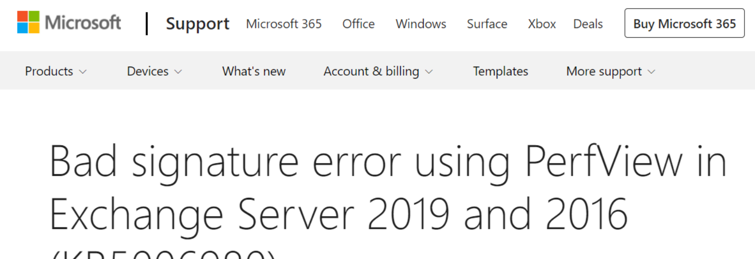
Automation

SA SaaS Integration

- ✓ Automatically analyze new versions
- ✓ Analysis history
- ✓ Re-analysis on emergent threats
- ✓ Alerting on risks

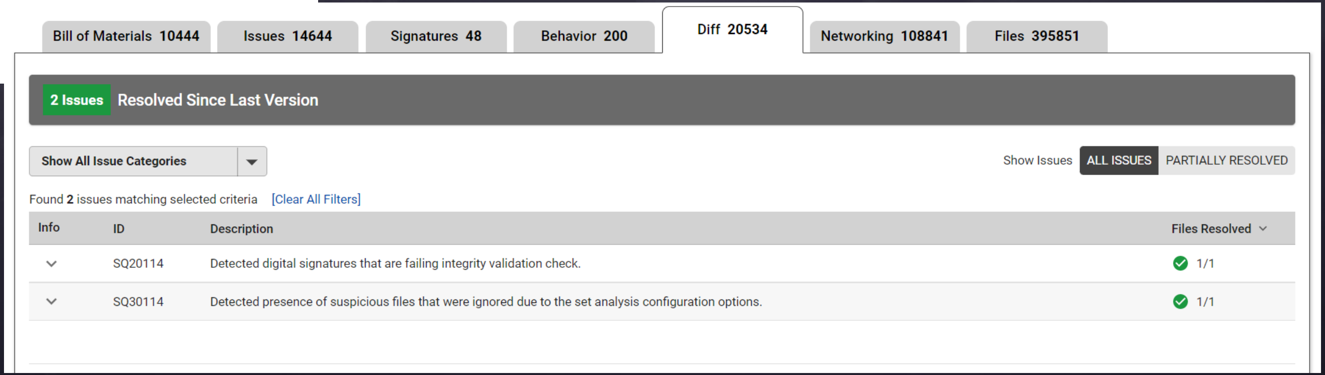
Demo - Differential analysis

ExchangeServer2016-x64-CU22.ISO


Microsoft | Support Microsoft 365 Office Windows Surface Xbox Deals Buy Microsoft 365
Products Devices What's new Account & billing Templates More support

Bad signature error using PerfView in Exchange Server 2019 and 2016 (KB5006980)

Exchange Server 2019, Exchange Server 2016



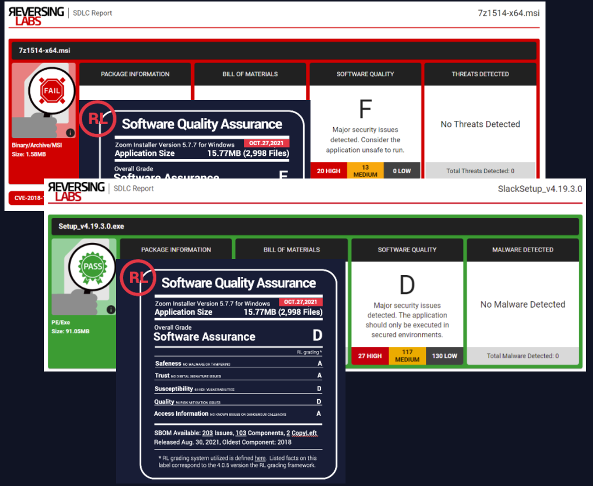
2 Issues Resolved Since Last Version

Found **2** issues matching selected criteria

Info	ID	Description	Files Resolved
	SQ20114	Detected digital signatures that are failing integrity validation check.	✓ 1/1
	SQ30114	Detected presence of suspicious files that were ignored due to the set analysis configuration options.	✓ 1/1

Shoring Software Assurance

MANAGED SERVICE FOR COMMERCIAL SOFTWARE AND OPEN SOURCE



ЯEVERSING LABS | SDLC Report 7z1514-x64.msi

7z1514-x64.msi

FAIL

Binary/Archive/MSI
Size: 1.58MB

CVE-2018-

PACKAGE INFORMATION | BILL OF MATERIALS | SOFTWARE QUALITY | THREATS DETECTED

Software Quality Assurance

Zoom Installer Version 5.7.7 for Windows OCT.27,2021
Application Size 15.77MB (2,998 Files)

Overall Grade
Software Assurance F

F

Major security issues detected. Consider the application unsafe to run.

20 HIGH 13 MEDIUM 0 LOW

No Threats Detected

Total Threats Detected: 0

ЯEVERSING LABS | SDLC Report SlackSetup_v4.19.3.0

Setup_v4.19.3.0.exe

PASS

PE/Exe
Size: 91.05MB

PACKAGE INFORMATION | BILL OF MATERIALS | SOFTWARE QUALITY | MALWARE DETECTED

Software Quality Assurance

Zoom Installer Version 5.7.7 for Windows OCT.27,2021
Application Size 15.77MB (2,998 Files)

Overall Grade
Software Assurance D

RL grading*

Safeness NO MALWARE OR TAMPERING	A
Trust NO DIGITAL SIGNATURE ISSUES	A
Susceptibility 6 HIGH VULNERABILITIES	D
Quality 94 RISK MITIGATION ISSUES	D
Access Information NO KNOWN ISSUES OR DANGEROUS CALLBACKS	A

SBOM Available: 203 Issues, 103 Components, 2 CopyLeft
Released Aug. 30, 2021, Oldest Component: 2018

* RL grading system utilized is defined here. Listed facts on this label correspond to the 4.0.5 version the RL grading framework.

D

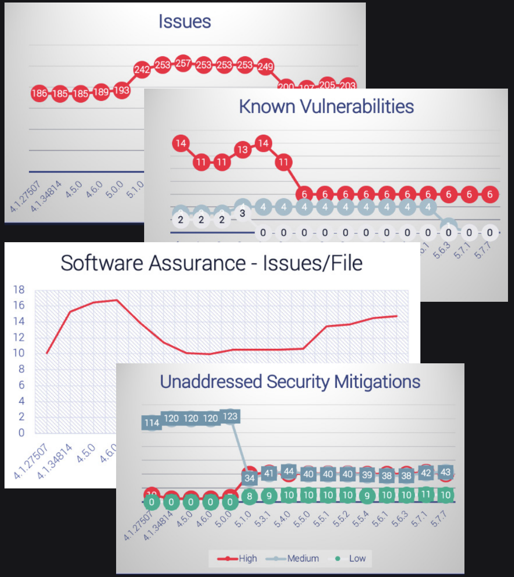
Major security issues detected. The application should only be executed in secured environments.

27 HIGH 117 MEDIUM 130 LOW

No Malware Detected

Total Malware Detected: 0

APPLICATION MONITORING MANAGED SERVICE FOR COMMERCIAL SOFTWARE AND OPEN SOURCE



ON-PREMISE SOFTWARE INSPECTION INFRASTRUCTURE

Malware and Software Integrity Inspection for Air-Gapped Networks and On-Premises Deployment

Summary

- Emerging supply chain attacks require a new approach
  - Decompose and analyze deployment image
- Determine software risk
  - Verified components
  - Mitigated vulnerabilities
  - Trustworthy behaviors
  - Protected secrets
  - Differential analysis
- Implement a continuous process for all releases

Questions?

- **Secure.software powered by ReversingLabs**

  https://www.secure.software/

secure.software
POWERED BY REVERSINGLABS

- **SolarWinds - SunBurst: the next level of stealth**

  https://blog.secure.software/sunburst-the-next-level-of-stealth

- **Codecov - It only takes one line of code to ruin your day**

  https://blog.secure.software/it-only-takes-one-line-of-code-to-ruin-your-day

- **Groundhog day: NPM package caught stealing browser passwords**

  https://blog.secure.software/groundhog-day-npm-package-caught-stealing-browser-passwords

- **Contact us to schedule a Demo!**

  https://register.reversinglabs.com/demo

GET STARTED

About Carahsoft

Carahsoft Technology Corp. is a trusted government IT solutions provider. The company combines technological expertise with a thorough understanding of the government procurement process to help Federal, State and Local Government agencies select and implement the best solution at the best possible value.

Need a government buying vehicle?

Carahsoft holds numerous contracts on behalf of ReversingLabs which makes the buying process easy.

For a list of Federal, State and Local buying vehicles see the Carahsoft site here.

For more information on ReversingLabs solutions, contact:

Reem Lakkis
The ReversingLabs Team at
Carahsoft Technology Corp.
703-581-6717 (Direct)
reem.lakkis@carahsoft.com
www.carahsoft.com/reversinglabs

For more information on ReversingLabs products for your agency, please contact: **866-421-4683**

REVERSINGLABS

Thank you

erik.thoen@reversinglabs.com

in linkedin.com/**in/erikthoen**

reversinglabs.com