Securing the software supply chain

They're coming for your code.
Learn about the rising cybersecurity risk to the software supply chain and what you can do!

The reality of software supply chain risk

1 in 8

open source downloads have known risk[1]

18.6%

of open source Java and JavaScript projects that were maintained in 2022 are no longer maintained today[2]

96%

of vulnerable downloaded releases had a fixed version available[3]

Overall, attacks fall into three categories:

1. Compromising the development pipeline
2. Exploiting the software operations pipeline
3. Vulnerabilities in subcomponents or dependencies

A multi-prong approach to defense

1. Use people and processes, not just technology

Embrace a culture of cybersecurity and employ processes that form the foundation of a secure software supply chain.

2. Produce high-quality software

Ensure vulnerabilities are quickly detected before software is deployed and patches are applied in a timely manner.

3. Protect the software development pipeline

Go beyond a pipeline designed to catch inadvertent vulnerabilities and adopt a resilient approach designed to detect changes by untrusted actors.

4. Respond quickly to vulnerabilities

Have a process in place to quickly identify, confirm, and remediate vulnerabilities.

Secure the software supply chain with OpenText™ Fortify™

Learn more

opentext.com

Fortify by opentext™

[1] Sonatype, *2023 Sonatype State of the Software Supply Chain*
[2] Ibid.
[3] Ibid.

Copyright © 2024 Open Text. All Rights Reserved. Trademarks owned by Open Text.
For more information, visit: https://www.opentext.com/about/copyright-information • 236-000024-001 | 07.24