Contrast SECURITY

4 Ways to Boost Application Security this Month

Lives and businesses can be disrupted when cyber criminals exploit vulnerabilities in the tools we rely on every day. According to Verizon, compromised applications remain a primary pathway for successful attacks—representing 39% of all data breaches in the last year.[1]

Contrast is proud to be a 2021 Champion for Cybersecurity Awareness Month—helping to promote global awareness of online safety and privacy. This annual campaign is a global effort between businesses, government agencies, colleges and universities, associations, nonprofit organizations, and individuals—designed to raise awareness and help everyone stay safer online.

President Biden's executive order on "improving the nation's cybersecurity (14028)" focuses largely on application security.

Four Application Security Practices You Should Start Today

Application security should not be an afterthought or an optional value-add. It needs to be a prioritized part of the culture—something that is built into all products and processes. Following are four things that developers and security teams can do this month to improve their approach to application security.

GENERATE A SECURITY BILL OF MATERIALS

Application security should extend from pre-development through production and include secure design and in-application protection.

As part of these efforts, organizations should generate a **software bill of materials (SBOM)** for all applications. SBOMs are a centerpiece of President Biden's recent Cybersecurity Executive Order.[2] While SBOMs are now mandated for federal agencies, many private companies are also starting to require SBOMs—especially in heavily regulated sectors such as healthcare and finance. SBOMs should encompass both open-source and custom code.

START BUILDING THREAT MODELS

Threat modeling is required by standards for the National Institute of Standards and Technology (NIST) and Payment Card Industry (PCI) and now with the Open Web Application Security Project (OWASP) Top Ten from 2021. A critical starting point is to read the Threat Modeling Manifesto that addresses questions such as what are we working on, what can go wrong, what are we going to do about it, and did we do a good enough job.[3]

Threat modeling helps organizations proactively visualize and identify potential application threats. They can be employed both before and after a line of code has been written.[4] This allows developers and security teams to avoid mistakes and build security into an organization's culture by informing decisions across design, development, testing, and operations.

Contrast SECURITY

START MEASURING TIME TO REMEDIATE AND VELOCITY OF INTRODUCING VULNERABILITIES

Plotting a course toward improved application security starts by knowing where you are today. There are some key metrics that can help keep efforts on course.

- Tracking mean time to remediation (MTTR) can help you understand how well you are shifting left—fixing issues earlier in the development cycle, where repairs are easier and cheaper to make. Organizations can detect and fix true vulnerabilities more quickly (and reduce MTTR) by implementing frictionless security testing tools with low false positives.[5]

- Calculating your vulnerability escape rate (VER) provides a simple metric to help the organization understand how many vulnerabilities are escaping the development process over a given period. "Just-in-time" security training empowers developers with the ability to fix vulnerabilities in their processes, which helps lower VER.[6]

PROTECT YOUR SOFTWARE SUPPLY CHAIN

Successful attacks on the software supply chain such as SolarWinds, Kaseya, and Microsoft Exchange Server over the past year demonstrate the risk vulnerabilities can pose. The SolarWinds exploit was the result of a build tool hack—which ultimately affected tens of thousands of organizations.[7] Kaseya was the result of known vulnerabilities that were not remediated before cyber criminals were able to gain access to roughly 50 managed service providers (MSPs) and spread to around 1,500 of their customers worldwide. Microsoft Exchange Server was the result of four zero-day vulnerabilities that were quickly exploited by multinational nation-state bad actors and used to gain access to thousands of users.

There are four security dimensions in the software supply chain: a) software you write, b) software you import, c) software you run, and d) software you build with.[8] Securing each dimension is crucial to protect against attacks on the software supply chain.

"Do Your Part. #BeCyberSmart."

If everyone does their part—implementing stronger security practices, raising awareness, and educating vulnerable audiences—our interconnected world will be safer and more secure for everyone. For more information about Cybersecurity Awareness Month 2021 and how to participate in a wide variety of activities, visit staysafeonline.org/cybersecurity-awareness-month/. You can also follow the official hashtag **#BeCyberSmart** on social media.

Contrast SECURITY

[1] "2021 Data Breach Investigations Report," Verizon, May 2021.
[2] "Executive Order on Improving the Nation's Cybersecurity," The White House, May 12, 2021.
[3] "Threat Modeling Manifesto," accessed October 8, 2021.
[4] Adam Shostack, "NIST Brings Threat Modeling into the Spotlight," Dark Reading, September 23, 2021.
[5] Jeff Williams, "How To Start Decluttering Application Security," Forbes, January 27, 2021.
[6] Jeff Williams, "Why You Should Consider Just-In-Time Training For Developers," Forbes, September 16, 2021.
[7] Saheed Oladimeji and Sean Michael Kerner, "SolarWinds hack explained: Everything you need to know," TechTarget, June 16, 2021.
[8] "4 Dimensions of Modern Application Security," Contrast Security, June 2021.

Contrast Security provides the industry's most modern and comprehensive Application Security Platform, removing security roadblocks inefficiencies and empowering enterprises to write and release secure application code faster. Embedding code analysis and attack prevention directly into software with instrumentation, the Contrast platform automatically detects vulnerabilities while developers write code, eliminates false positives, and provides context-specific how-to-fix guidance for easy and fast vulnerability remediation. Doing so enables application and development teams to collaborate more effectively and to innovate faster while accelerating digital transformation initiatives. This is why a growing number of the world's largest private and public sector organizations rely on Contrast to secure their applications in development and extend protection in production.

240 3rd Street
2nd Floor
Los Altos, CA 94022
Phone: 888.371.1333
Fax: 650.397.4133

Contrast SECURITY

contrastsecurity.com