

IS OUR WORLD SECURE YET? (ARE WE EVEN CLOSE?) : *AN UPDATE ON CISA'S SECURE BY DESIGN INITIATIVE*

KIRK LAWRENCE



Introduction

Secure by Design Is Hard



Background

In the past 18 months, CISA has...

1. Preached the gospel of Secure by Design
2. Released the Secure by Design Pledge
3. Published 6 Secure by Design Alerts and 11 Secure by Design Blogs
4. Established a Working Group with CISA to coordinate SbD activities across 8 disparate workstreams.
5. Continue to advance Software Bill-of-Materials (SBOM) adoption across the USG and internationally, focusing on scaling and operationalizing SBOM tools to improve visibility into software products.
6. Published an Open Source Software Security Roadmap that lays out our priorities for securing the open source software ecosystem. Worked to increase broad understanding of SbD principles in OS SW use and development.



Principles

1. Manufacturers should take ownership of the security **outcomes** for their customers. The burden of safety should never fall solely upon the customer.
2. Manufacturers should embrace **radical transparency** and accountability.
3. Manufacturers should build **organization structure** and leadership to ensure safety is built in.





SECURE BY DESIGN

PLEDGE

Within a year, demonstrate measurable progress in the following areas:

1. Increase the use of multi-factor authentication (MFA).
2. Reduce default passwords across products.
3. Reduce entire classes of vulnerabilities.
4. Increase the installation of security patches by customers.
5. Publish a vulnerability disclosure policy (VDP).
6. Transparency in vulnerability reporting. (CVE)
7. Increase in the ability for customers to gather evidence of intrusions.



Secure by Demand

CISA Goal:

Offer resources that organizations can leverage to assess product security maturity that aligns with our Secure by Design Principles.



CISA'S SbD Impact

Have we made the world more secure?

~_(\ツ)_/~



Call to Action

1. Don't lose sight of the goal and don't lose faith.
2. Be an Advocate.
3. Celebrate the Mundane.
4. Contribute to the Data Set.





Questions?

Email:
securebydesign@cisa.dhs.gov

