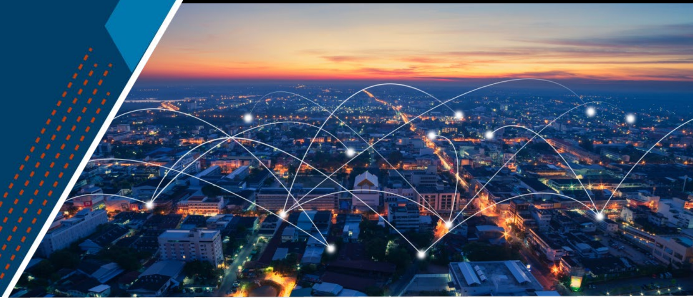
Secure by Design Alert

How Software Manufacturers Can Shield Web Management Interfaces From Malicious Cyber Activity



Malicious Cyber Activity Against Vulnerable Web Management Interfaces

Malicious cyber actors continue to find and exploit vulnerabilities in web management interfaces. In response, software manufacturers continue to ask why customers did not harden their products to avoid such incidents.

Secure by Design Lessons to Learn

"Secure by design" means that software manufacturers build their products in a way that reasonably protects against malicious cyber actors successfully exploiting vulnerabilities in their products. Baking in this risk mitigation, in turn, reduces the burden of cybersecurity on customers. Exploitation of vulnerabilities in web management interfaces continues to cause significant harm to organizations around the world—but can be avoided at scale. CISA urges software manufacturers to learn from ongoing malicious cyber activity against web management interfaces by reviewing the principles below.

Principle 1: Take Ownership of Customer Security Outcomes

Principle 1 focuses on key areas where software manufacturers should invest in security: application hardening, application features, and default settings. When designing these areas, software manufacturers should **examine the default settings of their products**. For instance, if it is a known best practice to shield a system from the public internet, do not rely on customers to do so. Rather, have the **product itself** enforce security best practices. Examples include:

- Disabling the product's web interface by default and including a "loosening guide" that lists the risks—in both technical and non-technical language—that come with making changes to the default configurations.[i]
- Configuring the product so that it does not operate while in a vulnerable state, such as when the product is directly exposed to the internet.
- Warning the administrator that changing the default behavior may introduce significant risk to the organization.

Additionally, software manufacturers should conduct field tests to understand how their customers deploy products in their unique environments and whether customers are deploying products in unsafe ways. This practice will help bridge the gap between developer expectations and actual customer usage of the product. Field tests will help identify ways to build the product so customers will securely use it.

Furthermore, software manufacturers should consistently enforce authentication throughout their product, especially on critical interfaces such as administrator portals.

Principle 2: Embrace Radical Transparency and Accountability

Software manufacturers should lead with transparency when disclosing product vulnerabilities. To that end, manufacturers should track the root cause of vulnerabilities and ensure CVE entries are complete and include the proper CWE field denoting the class of coding error that led to the vulnerability. Not only does this help customers understand and assess risk, but it also enables other software manufacturers to learn from mistakes fixed across the industry.

Finally, software manufacturers should look to identify—and take action to eliminate—repeat classes of vulnerabilities in products.

This document is marked TLP:CLEAR: Recipients may share TLP:CLEAR information without restriction. Information is subject to standard copyright rules. For more information on the Traffic Light Protocol, see https://www.cisa.gov/tlp.

As of Nov. 29, 2023

For more information, review Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Secure by Design Software.

Action Item for Software Manufacturers

To shield their customers from malicious cyber activity targeting web management interfaces, software manufacturers should adopt the principles set forth in Shifting the Balance of Cybersecurity Risk and publish their own secure-by-design roadmap that demonstrates that they are not simply implementing tactical controls but are rethinking their role in keeping customers secure.

[i] There have been multiple Known Exploited Vulnerabilities (KEVs) involving management interfaces and, especially, the web-enabled versions. For example, CISA added the following vulnerabilities to the KEV Catalog this year: CVE-2023-20198, CVE-2017-6884, CVE-2023-38035, CVE-2019-17621, which affect web management interfaces on Cisco, Zyxel, Ivanti, and D-Link products, respectively.