Product Security Bad Practices

Publication: October 2024

Cybersecurity and Infrastructure Security Agency

Federal Bureau of Investigation

Table of Contents

Overview

As outlined in CISA's Secure by Design initiative, software manufacturers should ensure that security is a core consideration from the onset of software development. This voluntary guidance provides an overview of product security bad practices that are deemed exceptionally risky, particularly for software manufacturers who produce software used in service of critical infrastructure or national critical functions (NCFs) and provides recommendations for software manufacturers to mitigate these risks.

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) and the Federal Bureau of Investigation (FBI) (hereafter referred to as the authoring organizations) developed this guidance to urge software manufacturers to reduce customer risk by prioritizing security throughout the product development process. This document is intended for software manufacturers who develop software products and services—including on-premises software, cloud services, and software as a service (SaaS)—used in support of critical infrastructure or NCFs. The authoring organizations strongly encourage all software manufacturers to avoid these product security bad practices. By following the recommendations in this guidance, manufacturers will signal to customers that they are taking ownership of customer security outcomes, a key Secure by Design principle. The guidance contained in this document is non-binding and while CISA encourages organizations to avoid these bad practices, this document imposes no requirement on them to do so.

The bad practices are divided into three categories.

1. Product properties, which describe the observable, security-related qualities of a software product.
2. Security features, which describe the security functionalities that a product supports.
3. Organizational processes and policies, which describe the actions taken by a software manufacturer to ensure strong transparency in its approach to security.

This list is focused and does not include every possible inadvisable cybersecurity practice. The lack of inclusion of any particular cybersecurity practice does not indicate that CISA endorses such a practice or deems such a practice to present acceptable levels of risk. Items present in this list were chosen based on the threat landscape as representing the most dangerous and pressing bad practices that software manufacturers should avoid.

Product Properties

Development in Memory Unsafe Languages (CWE[1]-119 and related weaknesses)

The development of new product lines for use in service of critical infrastructure or NCFs in a memory-unsafe language (e.g., C or C++) where there are readily available alternative memory-safe

[1] Common Weakness Enumeration.

languages that could be used is dangerous and significantly elevates risk to national security, national economic security, and national public health and safety.

For existing products that are written in memory-unsafe languages, not having a published memory safety roadmap by January 1, 2026 is dangerous and significantly elevates risk to national security, national economic security, and national public health and safety. The memory safety roadmap should outline the manufacturer's prioritized approach to eliminating memory safety vulnerabilities in priority code components (e.g., network-facing code or code that handles sensitive functions like cryptographic operations). Manufacturers should demonstrate that the memory safety roadmap will lead to a significant, prioritized reduction of memory safety vulnerabilities in the manufacturer's products and demonstrate they are making a reasonable effort to follow the memory safety roadmap. This does not apply to products that have an announced end-of-support date that is prior to January 1, 2030.

Recommended action: Software manufacturers should build products in a manner that systematically prevents the introduction of memory safety vulnerabilities, such as by using a memory safe language or hardware capabilities that prevent memory safety vulnerabilities. Additionally, software manufacturers should publish a memory safety roadmap by January 1, 2026.

Resources: The Case for Memory Safe Roadmaps, CISA Secure by Design Pledge (Reducing Classes of Vulnerability), Back to The Building Blocks, NIST Secure Software Development Framework (SSDF) PW 6.1.

Inclusion of User-Provided Input in SQL Query Strings (CWE-89)

The inclusion of user-provided input directly in the raw contents of a SQL database query string in products used in service of critical infrastructure or NCFs is dangerous and significantly elevates risk to national security, national economic security, and national public health and safety.

Recommended action: Products should be built in a manner that systematically prevents the introduction of SQL injection vulnerabilities, such as by consistently enforcing the use of parametrized queries.

Resources: CISA Secure by Design Pledge (Reducing Classes of Vulnerability), SSDF PW.5.1, CISA SQL Injection Secure by Design Alert.

Inclusion of User-Provided Input in Operating System Command Strings (CWE-78)

The inclusion of user-provided input directly in the raw contents of an operating system command string in products used in service of critical infrastructure or NCFs is dangerous and significantly elevates risk to national security, national economic security, and national public health and safety.

Recommended action: Software manufacturers should build products in a manner that systematically prevents command injection vulnerabilities, such as by consistently ensuring that command inputs are clearly delineated from the contents of a command itself.

Resources: CISA Secure by Design Pledge (Reducing Classes of Vulnerability), SSDF PW.5.1.

Presence of Default Passwords (CWE-1392 and CWE-1393)

The release of a product used in service of critical infrastructure or NCFs with default passwords, which CISA defines as universally-shared passwords that are present by default across a product, is dangerous and significantly elevates risk to national security, national economic security, and national public health and safety.

Recommended action: Software manufacturers should ensure that default passwords are not present in a product, such as by:

- Providing random, instance-unique initial passwords for the product.
- Requiring the user installing the product to create a strong password at the start of the installation process.
- Providing time-limited setup passwords that disable themselves when a setup process is complete and require configuration of a secure password (or more secure authentication approaches, such as phishing-resistant MFA).
- Requiring physical access for initial setup and the specification of instance-unique credentials.
- Conducting campaigns or offering updates that transition existing deployments from default passwords to more secure authentication mechanisms.

Resources: CISA Secure by Design Pledge (Default Passwords), SSDF PW.9.1, CISA Default Passwords Secure by Design Alert.

Presence of Known Exploited Vulnerabilities

The release of a product used in service of critical infrastructure or NCFs that, at time of release, includes a component that contains an exploitable vulnerability present on CISA's Known Exploited Vulnerabilities (KEV) Catalog is dangerous and significantly elevates risk to national security, national economic security, and national public health and safety. Additionally, if a new KEV affecting the product is published in CISA's catalog, failure to issue a patch at no cost to its users in a timely manner if the KEV is exploitable in the product or failure to publicly document the presence of the vulnerability if the KEV is not exploitable in the product, is dangerous and significantly elevates risk to national security, national economic security, and national public health and safety.

Recommended action: Software manufacturers should patch all known exploited vulnerabilities within software components prior to release. In the case of the publication of a new KEV on CISA's catalog, the manufacturer should issue a patch at no cost to its users in a timely manner (under no circumstances longer than 30 days) and clearly warn users of the associated risks of not installing the patch.

If the manufacturer deems that a KEV cannot be exploited in its product (because, for instance, the KEV is only exploitable via a function that is never called), the manufacturer should publicly publish

written documentation acknowledging the KEV and explaining how it is not exploitable in their product.[2]

Resources: CISA Secure by Design Pledge (Security Patches), SSDF PW.4.4, Binding Operational Directive 22-01.

Presence of Open Source Software with Known Exploitable Vulnerabilities

The release of a product used in service of critical infrastructure or NCFs that, at time of release, includes open source software components that have known exploitable vulnerabilities is dangerous and significantly elevates risk to national security, national economic security, and national public health and safety.[3] Additionally, if exploitable vulnerabilities are subsequently disclosed in the included open source components, failure to issue a patch or other mitigation at no cost to the product's users in a timely manner is dangerous and significantly elevates risk to national security, national economic security, and national public health and safety.

Recommended action: Software manufacturers should responsibly consume and sustainably contribute to the open source software that they depend on. This includes making a reasonable effort to evaluate and secure their open source software dependencies by taking the following actions: [4]

- Maintaining a software bill of materials (SBOM) describing all first- and third-party software dependencies, both open source and proprietary, and being able to provide this to customers.
- Having an established process for managing the incorporation of open source software, including taking reasonable steps to:
    - Run security scanning tools on each open source software component when selected, including its dependencies and transitive dependencies, and each subsequent version when updated.
    - Select open source software projects that are well-maintained, and—when appropriate—contribute to the project's ongoing maintenance to sustain the expected standard of quality.
    - Evaluate alternatives to identify and select the most well-secured and maintained option.
    - Download open source software project artifacts from package repositories (or other appropriate sources) that adhere to security best practices.
    - Routinely monitor for Common Vulnerabilities and Exposures (CVEs) or other security-relevant alerts, such as end-of-life, in all open source software dependencies and update them as necessary.

[2] Ideally, the documentation should be published in a machine-processable format through Vulnerability Exploitability eXchange (VEX).
[3] Critical vulnerabilities are defined as those with a Common Vulnerability Scoring System (CVSS) score of 9.0 or greater.
[4] Organizations may choose to establish an open source program office (OSPO) to centralize these activities.

  - Cache copies of all open-source dependencies within the manufacturer's own build systems and do not update products or customer systems directly from unverified public sources.
- Including the cost of updating to new major versions of third-party open source software dependencies in business planning activities and ensuring that such dependencies continue to receive necessary security fixes for the expected product life.

Resources: SSDF PW.4.4, ESF Recommended Practices for Managing Open Source Software and Software Bill of Materials, TODO Group Open Source Program Office (OSPO) Definition and Guide.

Security Features

Lack of Multifactor Authentication

For products used in service of critical infrastructure or NCFs that authenticate users not supporting multi-factor authentication (MFA) in the baseline version of the product is dangerous and significantly elevates risk to national security, national economic security, and national public health and safety.

Additionally, products that do not enable MFA by default for administrator accounts after January 1, 2026 are dangerous and significantly elevate risk to national security, national economic security, and national public health and safety. This does not apply to products that have an announced end-of-support date that is prior to January 1, 2028.

Recommend action: Software manufacturers should either support MFA natively in the product (if the product itself handles authentication) or support in the baseline version of the product the use of an external identity provider, such as via single sign on. Require MFA for administrators.

Resources: CISA Secure by Design Pledge (Multi-Factor Authentication), SSDF PW.9.

Lack of Capability to Gather Evidence of Intrusions

For products used in service of critical infrastructure or NCFs, it is dangerous and significantly elevates risk to national security, national economic security, and national public health and safety to not provide customers with artifacts and capabilities in the baseline version of the product sufficient to gather evidence of common forms of intrusions affecting the product, which at minimum includes:

- Configuration changes or reading configuration settings;
- Identity (e.g., sign-in and token creation) and network flows, if applicable; and
- Data access or creation of business-relevant data.

Recommended action:

- As part of the baseline version of a product, software manufacturers should make logs available in an industry-standard format related to, at minimum, the above listed areas.

- For cloud service providers and SaaS products, software manufacturers should retain logs for a set timeframe (at least 6 months) at no additional charge.

Resources: CISA Secure by Design Pledge (Evidence of Intrusions).

Organizational Processes and Policies

Failing to Publish Timely CVEs with CWEs

For products used in service of critical infrastructure or NCFs, it is dangerous and significantly elevates risk to national security, national economic security, and national public health and safety for the software manufacturer to not issue CVEs in a timely manner for, at minimum, all critical or high impact vulnerabilities (whether discovered internally or by a third party). Additionally, it is dangerous and significantly elevates risk to national security, national economic security, and national public health and safety to not include the CWE field in every CVE record.

Recommended action: Software manufacturers should publish complete CVEs, including the appropriate CWE field, in a timely manner for all critical or high impact vulnerabilities.

Resources: CISA Secure by Design Pledge (CVEs), SSDF RV.1.3.

Failing to Publish a Vulnerability Disclosure Policy

For products used in service of critical infrastructure or NCFs, not having a published vulnerability disclosure policy (VDP) that includes the product in its scope is dangerous and significantly elevates risk to national security, national economic security, and national public health and safety.

Recommended actions:

- Software manufacturers should publish a VDP that:
  - Authorizes testing by members of the public on products offered by the manufacturer;
  - Commits to not recommending or pursuing legal action against anyone engaging in good faith efforts to follow the VDP,
  - Provides a clear channel to report vulnerabilities; and
  - Allows for public disclosure of vulnerabilities in line with coordinated vulnerability disclosure (CVD) best practices and international standards.
- Software manufacturers should remediate all valid reported vulnerabilities in a timely and risk-prioritized manner.

Resources: CISA Secure by Design Pledge (Vulnerability Disclosure Policy), SSDF RV.1.3, ISO 29147.