December 13, 2024

Cybersecurity and Infrastructure Security Agency (CISA)
Department of Homeland Security
1110 N. Glebe Road
Arlington, VA 20598-0630

Re: Comment on CISA's "Product Security Bad Practices" Document (Docket CISA-2024-0028)

Consumer Reports appreciates the chance to comment on CISA's product security bad practices guidance.

CR believes that the catalog provides strong recommendations for software manufacturers to avoid the bad practices outlined and work to mitigate the risks. We especially appreciate the inclusion of memory safety in software products listed alongside basic security features and a transparent approach to product security. Consumer Reports has been advocating for many of the measures listed since the launch of the Digital Standard in 2017[1].

We write to comment on some of the recommendations and add an additional layer to what has been discussed: a requirement for software companies and software as a service providers to include essential security features in their baseline products, even for its free or lowest cost tier.

Designing products that require a fee for fundamental security support (such as allowing administrators to set password complexity policies) that many small or medium sized businesses (SMBs) cannot afford is a bad — and arguably illegal — practice. It keeps organizations which are essential for consumer safety below the security poverty line[2]. And when those SMBs are hacked, it reduces trust in public and essential infrastructure, opens up avenues for malicious

[1] https://thedigitalstandard.org/
[2] Ellis, A. and Nather, W. "Living Below The Security Poverty Line: Coping Mechanisms" [Conference Presentation] RSA 2013. San Francisco. April 4-6. https://www.infosecuritymagazine.nl/files/2fb0642808f57f0f9831532ae8f7e8fd.pdf

actors to use SMB equipment for botnets, and can cause consumers considerable harm through the exposure of their private data as well as disrupting necessary services.

Over the past 19 years, the Federal Trade Commission has interpreted Section 5 of the FTC Act to mandate that companies use reasonable safeguards to protect services from external attacks that could access consumers' personal information.[3] Businesses should be required to abstain from offering products that do not meet these reasonable security mandates.

Memory Safety

We agree with these recommendations. Indeed, we called for memory safety roadmaps in 2023 in our memory safety convening report.[4] In the same report, we discussed new code as low hanging fruit and agree with your guidance for manufacturers to prevent introduction of memory safety vulnerabilities by using memory safe language or hardware capabilities to prevent them.

Presence of Default Passwords

We agree with this recommendation, and would like to see it strengthened by adding a stipulation requiring companies to allow administrators to set password complexity policies, such as password length, to resist brute force attempts, as we'll mention later on in this comment.

Lack of MFA

While we agree with guidance requiring NCFs to support MFA in their baseline products, and providing MFA by default for admin accounts, we'd further like to see products including a mechanism for administrators to mandate MFA by default for all users. We'd also like to see multiple forms of MFA offered beyond SMS-based MFA, given its inherent security risks.[5] These could include passkeys, as well as authentication apps and security keys.

Lack of Capability to Gather Evidence of Intrusions

---

[3] BJ's Wholesale Club Settles FTC Charges, https://www.ftc.gov/news-events/news/press-releases/2005/06/bjs-wholesale-club-settles-ftc-charges; DSW Inc. Settles FTC Charges | Federal Trade Commission, https://www.ftc.gov/news-events/news/press-releases/2005/12/dsw-inc-settles-ftc-charges; FTC Releases 2023 Privacy and Data Security Update, https://www.ftc.gov/news-events/news/press-releases/2024/03/ftc-releases-2023-privacy-data-security-update; Start with Security: A Guide for Business, https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf

[4] Yael Grauer. "Future of Memory Safety: Challenges and Recommendations." Consumer Reports. January 2023 https://innovation.consumerreports.org/Memory-Safety-Convening-Report-.pdf

[5] Implementing Phishing Resistant MFA." CISA, October 2022 https://www.cisa.gov/sites/default/files/2023-01/fact-sheet-implementing-phishing-resistant-mfa-508c.pdf

We agree with this guidance, though would recommend a 365-day retention period as well as specifying that export of audit logs should not require additional fees.

Failure to Publish a Vulnerability Disclosure Policy

Consumer Reports agrees with this guidance, and cautions that as software becomes a critical or even optional element in many everyday products, the makers of these products have neglected to consider the security best practices generally embraced by the enterprise IT world. For example, CR has conducted research showing how far the consumer IoT industry has to go in this respect.

In early 2024 CR conducted a study of 75 connected device brands and found that 28 percent didn't have a dedicated point of contact for security researchers.[6] A follow-on questionnaire found that 34 percent of those answering the survey didn't have a vulnerability disclosure program. The lack of these programs is possibly because many of these companies questioned were selling products such as vacuum cleaners, refrigerators, light bulbs, etc. that traditionally did not have anything to do with software and software security.

After CR reached out to ask about their vulnerability programs, four of the 75 companies made changes, and in two cases even created such a program. One company did not implement a VDP, but did add a dedicated point of contact for security researchers. This indicates that education and bringing the CISA pledge to more areas using software will provide rapid benefits.

Additional Topics

While the product properties, security features and organizational processes CISA is inquiring about in this comment are excellent, CR would like to propose some additional elements that we think will improve the quality of software everywhere, and thus boost national security and prevent harm to small businesses and consumers.

As an organization we have come out strongly in favor of the Zatik SaaS Safety Bar[7] as promulgated by Zatik Security. As an organization, CR has tirelessly advocated for manufacturers to include security features as a baseline. For example, CR has pushed for seatbelts in cars and automatic emergency braking as a standard feature in all new passenger vehicles. We are pushing for a similar set of security features for free and low-cost software.

---

[6] Stacey Higginbotham. "Who Ya' Gonna Call? Why IoT Companies Should Embrace Vulnerability Disclosure Programs." CR Innovation Lab Blog. July 29, 2024.
https://innovation.consumerreports.org/who-ya-gonna-call/

[7] Zak Glick, "Zatik SaaS Safety Bar. Zatik Security Blog. July 29, 202.
https://www.zatik.io/post/saas-safety-bar

These features are enumerated in the Zatik SaaS Safety Bar, which asks SaaS providers to do nine things:

- Include **support for multi-factor authentication** (MFA).
- Include an admin mechanism to **require all users to have MFA enabled.**
- Require **support for social sign-on (SSO) integration** via protocols such as SAML, with the ability for administrators to remove users and groups.
- Provide **basic role-based access control** to split administrative functions from those normal users have.
- Provide **an audit trail within the application** so administrators can identify actions taken by users, that should be retained for 365 days. If someone sends an invoice or modifies an item, there would be receipts. Some SaaS providers may not want to support data storage for an entire year for a free or lower tier account because the SaaS provider would have to fund the underlying cloud costs. We believe this could be addressed by allowing administrators to export the audit logs for free to S3 buckets, via syslogs, to AWS/GCP, and that the export must be ongoing so it could be loaded into an SIEM system. However Zatik Security CTO Zack Glick says he thinks exporting as a text file would meet the minimum bar.
- Provide a mechanism for **forced logout**, allowing admins to force users to log out of networks or to revoke their access, in case their account has been compromised, but without deleting the user altogether.
- **Allow administrators to set password complexity policies** (such as password length) to resist brute force attacks.
- Provide **encryption in transit (TLS).**
- Allow administrators to destroy data or have a **data destruction policy.**

Thank you for reviewing our comments. If you have any questions, please contact Yael Grauer at yael.grauer@consumer.org.

Respectfully,

Yael Grauer
Program Manager, Cybersecurity Research
Consumer Reports

Stacey Higginbotham
Policy Fellow
Consumer Reports

Justin Brookman
Director of Technology Policy
Consumer Reports