CLTC
Center for Long-Term Cybersecurity
UC Berkeley

Center for Long-Term Cybersecurity
University of California, Berkeley
102 South Hall #4600
Berkeley, CA 94720
https://cltc.berkeley.edu

To the the Cybersecurity and Infrastructure Security Agency (CISA) team developing guidance for Product Security Bad Practices,

The University of California, Berkeley Center for Long-Term Cybersecurity (CLTC) commends CISA for creating the Product Security Bad Practices list. After close review of the guidance, CLTC would like to offer support and recommendations specifically addressing the practices related to multi-factor authentication (MFA), as identified under the Security Features category.

MFA is a proven, simple, and effective tool for preventing unauthorized access and reducing the impact of cyber intrusions on organizations that are part of critical infrastructure and serve national critical functions (NCFs). According to CISA, requiring MFA for account access can lower the risk of account breaches by 99 percent. Its use should not be optional but *mandatory* in software products.

To summarize our positions, CLTC:

- Supports CISA's recommendation of offering MFA, specifically mandatory MFA for administrative accounts, as a minimum requirement for software manufacturers serving the nation's critical infrastructure;
- Recommends that CISA adapt the guidance to prioritize use of phishing-resistant MFA authentication methods, such asapp-based tokens or external hardware keys; and
- Recommends that, in addition to software manufacturers, identity providers such as single sign-on (SSO) companies should be subject to this guidance.

CLTC fully supports CISA's decision to identify ***Lack of Multifactor Authentication*** as a security bad practice for products serving the nation's critical infrastructure and NCFs. CLTC also agrees with CISA's recommendation that all software products with an end-of-support date after January 2028 should enable MFA by default for administrator accounts, as the absence of this security method poses significant risks to essential services and vulnerable communities.[1]

CLTC strongly supports the stance that software manufacturers must offer or support MFA in their products, either natively or via an external identity provider.

CLTC has two suggestions for how to improve CISA's Product Security Bad Practices guidance, specifically in the ***Security Features: Lack of Multifactor Authentication*** section:

[1] Leyden, John. "Authentication failure blamed for Change Healthcare ransomware attack." *CSO*, 23 Apr. 2024.

Recommendation #1: **CISA's guidance should prioritize phishing-resistant MFA authentication methods**

> Some methods of MFA are more vulnerable to phishing attacks, such as those based on email or SMS. We recommend that CISA's guidance prioritize phishing-resistant MFA authentication methods like app-based tokens or external hardware keys, by default. While phishing-resistant MFA is mentioned briefly in the ***Presence of Default Passwords*** section, CLTC recommends providing more explicit guidance in the ***Lack of Multifactor Authentication*** section to clarify the most secure authentication methods for software manufacturers.
>
> Approximately, 55 percent of all K-12 school data breaches between 2016 and 2021 were carried out on education technology vendors.[2] EdTech vendors have highlighted to us that K-12 schools often choose the least secure authentication methods, such as email and SMS-based MFA, when enabling MFA. By encouraging default MFA that integrates phishing-resistant methods, such as app-based tokens or hardware keys, software manufacturers can guide users towards stronger security practices and better protect them from evolving threats.

Recommendation #2: CISA should include identity providers in these guidelines

> Identity providers like single sign-on vendors (SSOs) play an important role in managing access for organizations using multiple software products. Some software manufacturers depend on identity providers to handle MFA instead of building it natively into their products. This dependence makes it very important for identity providers to uphold strong security standards, including by requiring MFA for privileged accounts. By addressing identity providers directly in this guidance, CISA can help ensure consistent and robust MFA implementation across organizations.

Thank you for your consideration of CLTC's recommendations, and for your leadership on product security.

Our best,

Shannon Pierson
Senior Fellow
Public-Interest Cybersecurity Program, The Center for Long-Term Cybersecurity, UC Berkeley

Sarah Powazek
Director
Public-Interest Cybersecurity Program, The Center for Long-Term Cybersecurity, UC Berkeley

[2] K12 SIX. "The State of K-12 Cybersecurity: Year in Review - 2022 Annual Report". 2022.