COST: **$**$$$ IMPACT: **MEDIUM** COMPLEXITY: **LOW**

2.N: Does the WWS disable Microsoft Office macros, or similar embedded code, by default on all assets?

Recommendation: Disable embedded macros and similar executable code by default on all assets.

Why is this control important?

By disabling macros by default, a WWS can reduce the risk from unauthorized executable code. Macros (i.e., embedded code) are software instructions contained within other files, such as Microsoft Office Word documents or Excel spreadsheets. Having these macros in a file can be helpful by automating repetitive tasks or updating data from online sources. However, attackers often use these macros to execute malicious code, download malware and viruses, or steal data.

An attacker can deliver a file with malicious macros to a WWS employee as an attachment to a phishing email. If the employee downloads the file, the macro within the file can leave your WWS's computer system vulnerable to breach, disruption, or damage.

Additional Guidance

- ✓ While a user can change this setting locally on individual assets, the WWS should implement it organization-wide through a system-enforced policy.
- ✓ The WWS should have a policy in place for authorized users to submit a request to enable macros. This request should justify the operational need for enabling macros so that the relevant OT/IT personnel or System Administrator can make their decision to allow or disallow the request based on the potential risk to WWS operations.

Implementation Tips

Disable macros by default on all OT and IT systems. When necessary for critical purposes, your WWS may enable macros on specific assets.

Resources

NIST 800-53 (Revision 5) Security and Privacy Controls for Information Systems and Organizations: See control SC-18 (page 311) for more information on managing macros, referred to as "Mobile Code". *https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final*

Microsoft Learn - Block macros from running in Office files from the Internet: See this resource for information on configuring Windows to block macros from the Internet. *https://learn.microsoft.com/en-us/deployoffice/security/internet-macros-blocked#block-macros-from-running-in-office-files-from-the-internet*