Microsoft is pleased to announce the release of the security baseline for Microsoft Edge, version 107!

We have reviewed the settings in Microsoft Edge version 107 and updated our guidance with the addition of one new setting. We're also highlighting three settings we would like you to consider based on your organizational needs. A new Microsoft Edge security baseline package was just released to the Download Center. You can download the new package from the Security Compliance Toolkit.

Spell checking provided by Microsoft Editor (Consider)
First introduced in Microsoft Edge, version 105. The Microsoft Editor utilizes the power of the cloud for enhanced spell checking for text fields within the browser. This feature securely transmits form data to a Microsoft service in the cloud, as described in the Microsoft Edge Privacy Whitepaper.. While the security baseline does not recommend a setting, customers should consider their own data privacy and security requirements. Further information on this setting can be found here.

Allow local MHTML files to open automatically in Internet Explorer mode (Consider)
Internet Explorer mode will remain a necessary option for the foreseeable future. However, it does come at a security cost. Any vulnerabilities in Internet Explorer will persist into the Internet Explorer mode session within Microsoft Edge. Therefore, if your organization doesn't require the use of MHTML files, then ensure you stay the most secure by disabling this setting. The security baseline will not yet enforce this setting as we understand many organizations are still in the transformation stage for many legacy applications. Further information on this setting can be found here.

Enhanced Security Mode configuration for Intranet zone sites (Consider)
This setting complements a setting we released in Microsoft Edge, version 98 (*Microsoft Edge\Enhance the security state of Microsoft Edge*). We still encourage you to test this setting and with the addition of this new Intranet Zone opt-out setting, enterprises now have the granular ability to opt-out Intranet sites making the feature (Enhanced Security Mode) easier to adopt. Further information on this setting can be found here.

Force WebSQL to be enabled (Disable)
WebSQL is a deprecated, non-standard, legacy feature that is destined to be removed from the web platform. The security baseline has explicitly disabled this policy setting; enterprises should plan to update any legacy applications that depend upon WebSQL. Further information on this setting can be found here.

Microsoft Edge version 107 introduced 12 new computer settings and 11 new user settings. We have included a spreadsheet listing the new settings in the release to make it easier for you to find them.

As a friendly reminder, all available settings for Microsoft Edge are documented here, and all available settings for Microsoft Edge Update are documented here.

Please continue to give us feedback through the Security Baseline Community or this post.