

Compatibilidade do mecanismo de prevenção de exploração da AMP para endpoints com EMET

Contents

[Introduction](#)

[Soluções](#)

Introduction

O EMET está incluído no Windows 10 e superior por padrão e está disponível como um complemento baixado para o Windows 7. Embora a Cisco não recomende a execução de mais de uma solução de proteção de memória ao mesmo tempo, há soluções alternativas que permitem que o componente de Prevenção de exploração do Cisco AMP para endpoints coexista com o EMET.

Soluções

- Para endpoints Windows 7, desative a regra EAF (Export Address Table Access Filtering, Filtragem de acesso à tabela de endereços de exportação) para processos protegidos pelo mecanismo de Prevenção de exploração do AMP para endpoints.
- Para endpoints Windows 10, desative as regras EAF (Export Address Table Access Filtering, Filtragem de Acesso à Tabela de Endereços de Exportação), IAF (Import Address Table Access Filtering, Filtragem de Acesso à Tabela de Endereços de Importação) e ACG (Arbitrary Code Guard) para processos protegidos pelo mecanismo AMP for Endpoints Exploit Prevention.