CAIS-Alerta: Resumo dos Boletins de Segurança da Microsoft - Maio/2016

[RNP, 12.05.2016]

A Microsoft publicou 16 boletins de segurança em 10 de maio de 2016 que abordam ao todo 37 vulnerabilidades em produtos da empresa. As explorações destas vulnerabilidades permitem **execução remota de código**, **elevação de privilégio**, **desvio de recurso de segurança**, **negação de serviço** e **divulgação não autorizada de informação**. Até o momento da publicação deste alerta não foram divulgados códigos de exploração para as vulnerabilidades listadas.

Severidade

Crítica

- MS16-051 - Atualização de segurança cumulativa para o Internet Explorer
- MS16-052 - Atualização de segurança cumulativa do Microsoft Edge
- MS16-053 - Atualização de segurança para JScript e VBScript
- MS16-054 - Atualização de segurança para o Microsoft Office
- MS16-055 - Atualização de segurança para o componente gráfico da Microsoft
- MS16-056 - Atualização de segurança do Diário do Windows
- MS16-057 - Atualizações de segurança para o Windows Shell
- MS16-064 - Atualização de segurança para o Adobe Flash Player

Importante

- MS16-058 - Atualização de segurança para o Windows IIS
- MS16-059 - Atualização de segurança para o Windows Media Center
- MS16-060 - Atualização de segurança para kernel do Windows
- MS16-061 - Atualização de segurança para RPC da Microsoft
- MS16-062 - Atualização de segurança para drivers do modo Kernel do Windows
- MS16-065 - Atualização de segurança para o .NET Framework
- MS16-066 - Atualização de segurança para o Modo de Segurança Virtual
- MS16-067 - Atualização de segurança para o Driver de Gerenciador de Volumes

Moderada

Nenhum boletim

Baixa

Nenhum boletim

O sistema de classificação de severidade das vulnerabilidades adotado pelo CAIS é o da própria Microsoft. O CAIS recomenda que se apliquem as correções para vulnerabilidades classificadas como crítica e importante. No caso de correções para vulnerabilidades classificadas como moderadas o CAIS recomenda que ao menos as recomendações de mitigação sejam seguidas.

- **Crítica** - Vulnerabilidades cuja exploração possa permitir a propagação de um worm sem a necessidade de interação com o usuário.
- **Importante** - Vulnerabilidades cuja exploração possa resultar no comprometimento de confidencialidade, integridade ou disponibilidade de dados de usuários ou a integridade ou disponibilidade de recursos de processamento.
- **Moderada** - exploração é mitigada significativamente por fatores como configuração padrão, auditoria ou dificuldade de exploração.
- **Baixa** - uma vulnerabilidade cuja exploração seja extremamente difícil ou cujo impacto seja mínimo.

Correções disponíveis

Recomenda-se atualizar os sistemas para as versões disponíveis em:
Microsoft Update
https://www.update.microsoft.com/microsoftupdate
Microsoft Download Center
http://www.microsoft.com/en-us/download/default.aspx

Mais informações

Resumo do Boletim de Segurança da Microsoft de maio de 2016
https://technet.microsoft.com/pt-br/library/security/ms16-may.aspx
Microsoft TechCenter de Segurança
https://technet.microsoft.com/pt-br/security
Microsoft Security Response Center – MSRC
https://technet.microsoft.com/pt-br/security/dn440717
Microsoft Security Research & Defense – MSRD
http://blogs.technet.com/b/srd/
Central de Proteção e Segurança Microsoft
https://www.microsoft.com/pt-br/security/default.aspx

Identificador CVE (http://cve.mitre.org):

CVE-2016-0187	CVE-2016-0193	CVE-2016-0169	CVE-2016- 0185	CVE-2016-0176
CVE-2016-0188	CVE-2016-0187	CVE-2016-0170	CVE-2016-0180	CVE-2016-0196
CVE-2016-0189	CVE-2016-0189	CVE-2016-0184	CVE-2016-0178	CVE-2016-0197
CVE-2016-0192	CVE-2016-0126	CVE-2016-0195	CVE-2016-0171	APSB16-15
CVE-2016-0194	CVE-2016-0140	CVE-2016-0182	CVE-2016-0173	CVE-2016-0149
CVE-2016-0186	CVE-2016-0183	CVE-2016-0179	CVE-2016-0174	CVE-2016-0181
CVE-2016-0191	CVE-2016-0198	CVE-2016-0152	CVE-2016- 0175	CVE-2016-0190
CVE-2016-0192	CVE-2016-0168			

O CAIS recomenda que os administradores mantenham seus sistemas e aplicativos sempre atualizados, de acordo com as últimas versões e correções oferecidas pelos fabricantes.
Os alertas do CAIS também são oferecidos no **Twitter**:

Siga @caisrnp