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

[RNP, 09.03.2016]

A Microsoft publicou 13 boletins de segurança em 8 de março de 2016 que abordam ao todo 36 vulnerabilidades em produtos da empresa. As explorações destas vulnerabilidades permitem **execução remota de código**, **elevação de privilégio** e **desvio de recurso de segurança**. Até o momento da publicação deste alerta não foram divulgados códigos de exploração para as vulnerabilidades listadas.

Severidade

Crítica

- MS16-023 - Atualização de segurança cumulativa para o Internet Explorer
- MS16-024 - Atualização de segurança cumulativa do Microsoft Edge
- MS16-026 - Atualização de segurança para fontes gráficas para corrigir a execução remota de código
- MS16-027 - Atualização de segurança do Windows Media para corrigir a execução remota de código
- MS16-028 - Atualização de segurança para a Biblioteca de PDF do Microsoft Windows para corrigir a execução remota de código

Importante

- MS16-025 - Atualização de segurança para o carregamento da biblioteca do Windows para corrigir execução remota de código
- MS16-029 - Atualização de segurança para Microsoft Office para corrigir a execução remota de código
- MS16-030 - Atualização de segurança para o Windows OLE para corrigir a execução remota de código
- MS16-031 - Atualização de segurança para o Microsoft Windows para corrigir a elevação de privilégio
- MS16-032 - Atualização de segurança para logon secundário para corrigir a elevação de privilégio
- MS16-033 - Atualização de segurança para o driver de classe de armazenamento em massa USB do Windows para corrigir a elevação de privilégio
- MS16-034 - Atualização de segurança dos drivers de modo kernel do Windows para corrigir a elevação de privilégio
- MS16-035 - Atualização de segurança para o .NET Framework para corrigir o bypass do recurso de segurança

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 março de 2016

https://technet.microsoft.com/pt-br/library/security/ms16-mar.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-2016-0102	CVE-2016-0111	CVE-2016-0116	CVE-2016-0098	CVE-2016-0087
CVE-2016-0103	CVE-2016-0112	CVE-2016-0123	CVE-2016-0101	CVE-2016-0099
CVE-2016-0104	CVE-2016-0113	CVE-2016-0124	CVE-2016-0117	CVE-2016-0133
CVE-2016-0105	CVE-2016-0114	CVE-2016-0125	CVE-2016-0118	CVE-2016-0093
CVE-2016-0106	CVE-2016-0102	CVE-2016-0129	CVE-2016-0021	CVE-2016-0094
CVE-2016-0107	CVE-2016-0105	CVE-2016-0130	CVE-2016-0057	CVE-2016-0095
CVE-2016-0108	CVE-2016-0109	CVE-2016-0100	CVE-2016-0134	CVE-2016-0096
CVE-2016-0109	CVE-2016-0110	CVE-2016-0120	CVE-2016-0091	CVE-2016-0132
CVE-2016-0110	CVE-2016-0111	CVE-2016-0121	CVE-2016-0092	

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