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

[RNP, 13.01.2016]

A Microsoft publicou 9 boletins de segurança em 12 de janeiro de 2016 que abordam ao todo 25 vulnerabilidades em produtos da empresa. As explorações destas vulnerabilidades permitem **execução remota de código**, **elevação de privilégio** e **falsificação**. Até o momento da publicação deste alerta não foram divulgados códigos de exploração para as vulnerabilidades listadas.

Severidade

Crítica

- MS16-001 - Atualização de Segurança Cumulativa para o Internet Explorer
- MS16-002 - Atualização de segurança cumulativa do Microsoft Edge
- MS16-003 - Atualização de segurança cumulativa para JScript e VBScript para corrigir execução remota de código
- MS16-004 - Atualização de segurança para o Microsoft Office para corrigir execução remota de código
- MS16-005 - Atualização de segurança para controladores do modo Kernel do Windows corrigir execução remota de código
- MS16-006 - Atualização de segurança do Silverlight para corrigir execução remota de código

Importante

- MS16-007 - Atualização de segurança para o Microsoft Windows para corrigir execução remota de código
- MS16-008 - Atualização de segurança do kernel do Windows para corrigir elevação de privilégio
- MS16-010 - Atualização de segurança no Microsoft Exchange Server para falsificação de endereços

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 janeiro de 2016

https://technet.microsoft.com/library/security/ms16-jan

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-2016-0002	CVE-2015-6117	CVE-2016-0008	CVE-2016-0016	CVE-2016-0007
CVE-2016-0005	CVE-2016-0010	CVE-2016-0009	CVE-2016-0018	CVE-2016-0029
CVE-2016-0003	CVE-2016-0011	CVE-2016-0034	CVE-2016-0019	CVE-2016-0030
CVE-2016-0024	CVE-2016-0012	CVE-2016-0014	CVE-2016-0020	CVE-2016-0031
CVE-2016-0002	CVE-2016-0035	CVE-2016-0015	CVE-2016-0006	CVE-2016-0032

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