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

[RNP, 11.02.2016]

A Microsoft publicou 13 boletins de segurança em 9 de fevereiro 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 **negação de serviço**. Até o momento da publicação deste alerta não foram divulgados códigos de exploração para as vulnerabilidades listadas.

**Severidade**

**Crítica**

- MS16-009 - Atualização de Segurança Cumulativa para o Internet Explorer
- MS16-011 - Atualização de segurança cumulativa do Microsoft Edge
- MS16-012 - Atualização de segurança para a biblioteca de PDF do Microsoft Windows para abordar a execução remota de código
- MS16-013 - Atualização de segurança para o Diário do Windows para abordar a execução remota de código
- MS16-015 - Atualização de segurança para o Microsoft Office para corrigir execução remota de código
- MS16-022 - Atualização de segurança para o Adobe Flash Player

**Importante**

- MS16-014 - Atualização de segurança para o Microsoft Windows para corrigir execução remota de código
- MS16-016 - Atualização de segurança do WebDAV para abordar elevação de privilégio
- MS16-017 - Atualização de segurança para driver de exibição da área de trabalho remota para abordar elevação de privilégio
- MS16-018 - Atualização de segurança dos drivers de modo kernel do Windows para corrigir elevação de privilégio
- MS16-019 - Atualização de segurança do .NET Framework para abordar negação de serviço
- MS16-020 - Atualização de segurança para Serviços de Federação do Active Directory para abordar negação de serviço
- MS16-021 - Atualização de segurança do servidor NPS RADIUS para abordar negação de serviço

**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 fevereiro de 2016

https://technet.microsoft.com/pt-br/library/security/ms16-feb.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-2016-0022 | CVE-2016-0042 | CVE-2016-0051 | CVE-2016-0059 | CVE-2016-0068 |
| CVE-2016-0033 | CVE-2016-0044 | CVE-2016-0052 | CVE-2016-0060 | CVE-2016-0069 |
| CVE-2016-0036 | CVE-2016-0046 | CVE-2016-0053 | CVE-2016-0061 | CVE-2016-0071 |
| CVE-2016-0037 | CVE-2016-0047 | CVE-2016-0054 | CVE-2016-0062 | CVE-2016-0072 |
| CVE-2016-0038 | CVE-2016-0048 | CVE-2016-0055 | CVE-2016-0063 | CVE-2016-0077 |
| CVE-2016-0039 | CVE-2016-0049 | CVE-2016-0056 | CVE-2016-0064 | CVE-2016-0080 |
| CVE-2016-0040 | CVE-2016-0050 | CVE-2016-0058 | CVE-2016-0067 | CVE-2016-0084 |
| CVE-2016-0041 | | | | |

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**