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

[RNP, 15.04.2016]

A Microsoft publicou 13 boletins de segurança em 12 de abril de 2016 que abordam ao todo 31 vulnerabilidades em produtos da empresa. As explorações destas vulnerabilidades permitem **execução remota de código**, **elevação de privilégio**, **desvio de recurso de segurança** e **negação de serviço**. Até o momento da publicação deste alerta não foram divulgados códigos de exploração para as vulnerabilidades listadas.

Severidade

Crítica

- MS16-037 - Atualização de segurança cumulativa para o Internet Explorer
- MS16-038 - Atualização de segurança cumulativa do Microsoft Edge
- MS16-039 - Atualização de segurança para o Microsoft Graphics Component
- MS16-040 - Atualização de segurança para Microsoft XML Core Services
- MS16-042 - Atualização de segurança para o Microsoft Office
- MS16-050 - Atualização de segurança para o Adobe Flash Player

Importante

- MS16-041 - Atualização de segurança para .NET Framework
- MS16-044 - Atualização de segurança para o Windows OLE
- MS16-045 - Atualização de segurança para o Windows Hyper-V
- MS16-046 - Atualização de segurança para o Logon secundário
- MS16-047 - Atualização de segurança para SAM e protocolos remotos LSAD
- MS16-048 - Atualização de segurança para CSRSS
- MS16-049 - Atualização de segurança para o HTTP.sys

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 abril de 2016
https://technet.microsoft.com/pt-br/library/security/ms16-Apr
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-2016-0154	CVE-2016-0154	CVE-2016-0143	CVE-2016-0122	CVE-2016-0089
CVE-2016-0159	CVE-2016- 0155	CVE-2016-0145	CVE-2016-0127	CVE-2016-0090
CVE-2016-0160	CVE-2016-0156	CVE-2016- 0165	CVE-2016-0136	CVE-2016-0135
CVE-2016-0162	CVE-2016-0157	CVE-2016-0167	CVE-2016-0139	CVE-2016-0128
CVE-2016-0164	CVE-2016-0158	CVE-2016-0147	CVE-2016-0153	CVE-2016-0151

CVE-2016-0166	CVE-2016-0161	CVE-2016-0148	CVE-2016-0088	CVE-2016-0150
APSB16-10				

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