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

[RNP, 14.06.2016]

A Microsoft publicou 16 boletins de segurança em 14 de junho de 2016 que abordam ao todo 44 vulnerabilidades em produtos da empresa. As explorações destas vulnerabilidades permitem **execução remota de código**, **elevação de privilégio**, **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

- MS16-063 - Atualização de segurança cumulativa para o Internet Explorer
- MS16-068 - Atualização de segurança cumulativa do Microsoft Edge
- MS16-069 - Atualização cumulativa de segurança para JScript e VBScript
- MS16-070 - Atualização de segurança para o Microsoft Office
- MS16-071 - Atualização de segurança para o servidor DNS do Microsoft Windows

Importante

- MS16-072 - Atualização de segurança para política de grupo
- MS16-073 - Atualização de segurança para drivers do modo Kernel do Windows
- MS16-074 - Atualização de segurança para o componente gráfico da Microsoft
- MS16-075 - Atualização de segurança para o servidor SMB do Windows
- MS16-076 - Atualização de segurança para Netlogon
- MS16-077 - Atualização de segurança para WPAD
- MS16-078 - Atualização de segurança para o Hub de Diagnóstico do Windows
- MS16-079 - Atualização de segurança para o Microsoft Exchange Server
- MS16-080 - Atualização de segurança para PDF no Microsoft Windows
- MS16-081 - Atualização de segurança para o Active Directory
- MS16-082 - Atualização de segurança para o componente de pesquisa do Microsoft Windows

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 junho de 2016
https://technet.microsoft.com/pt-br/library/security/ms16-jun
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-2016-0199	CVE-2016-3213	CVE-2016-3205	CVE-2016-3218	CVE-2016-3236
CVE-2016-0200	CVE-2016-3198	CVE-2016-3206	CVE-2016-3221	CVE-2016-3231
CVE-2016-3202	CVE-2016-3199	CVE-2016-3207	CVE-2016-3232	CVE-2016-0028
CVE-2016-3205	CVE-2016-3201	CVE-2016-0025	CVE-2016-3216	CVE-2016-3201
CVE-2016-3206	CVE-2016-3202	CVE-2016-3233	CVE-2016-3219	CVE-2016-3203
CVE-2016-3207	CVE-2016-3203	CVE-2016-3234	CVE-2016-3220	CVE-2016-3215
CVE-2016-3210	CVE-2016-3214	CVE-2016-3235	CVE-2016-3225	CVE-2016-3226
CVE-2016-3211	CVE-2016-3215	CVE-2016-3227	CVE-2016-3228	CVE-2016-3230
CVE-2016-3212	CVE-2016-3222	CVE-2016-3223	CVE-2016-3213	

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