**CAIS-Alerta: Resumo dos Boletins de Segurança Microsoft – Dezembro/2014**

[RNP, 12.12.2014]

A Microsoft publicou sete (7) boletins de segurança em 9 de dezembro de 2014, que abordam ao todo 25 vulnerabilidades em produtos da empresa. A exploração dessas vulnerabilidades permite a execução remota de código, elevação de privilégio e vazamento de informações. Até o momento da publicação desse alerta, não foram divulgados códigos de exploração para as vulnerabilidades listadas.

SEVERIDADE

. Crítica

- MS14-080: Atualização de segurança cumulativa para o Internet Explorer

- MS14-081: Vulnerabilidades no Microsoft Word e Microsoft Office Web Apps podem permitir a execução de código remoto

- MS14-084: Vulnerabilidade no mecanismo de script VBScript pode permitir execução remota de código

. Importante

- MS14-075: Vulnerabilidades no servidor do Microsoft Exchange podem permitir a elevação de privilégio

- MS14-082: Vulnerabilidade no Microsoft Office pode permitir a execução de código remoto

- MS14-083: Vulnerabilidades no Microsoft Excel pode permitir a execução remota de código

- MS14-085: Vulnerabilidade no componente do Microsoft Graphics pode permitir a divulgação de informações

. Moderada

- Nenhum boletim

. Baixa

- Nenhum boletim

O sistema de classificação de severidade das vulnerabilidades adotado pelo CAIS neste resumo é o da própria Microsoft. O CAIS recomenda que se aplique, minimamente, 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/pt-

br/download/default.aspx

MAIS INFORMAÇÕES

. Resumo do Boletim de Segurança da Microsoft de dezembro de 2014

https://technet.microsoft.com/library/security/ms14-dec

. Microsoft TechCenter de Segurança

http://technet.microsoft.com/pt-br/security/

. Microsoft Security Response Center - MSRC

http://www.microsoft.com/security/msrc/

. Microsoft Security Research & Defense - MSRD

http://blogs.technet.com/srd/

. Central de Proteção e Segurança Microsoft

http://www.microsoft.com/brasil/security/

Identificador CVE (http://cve.mitre.org<http://cve.mitre.org/>):

CVE-2014-6319, CVE-2014-6325, CVE-2014-6326, CVE-2014-6336, CVE-2014-6327, CVE-2014-6328, CVE-2014-6329, CVE-2014-6330, CVE-2014-6363, CVE-2014-6365, CVE-2014-6366, CVE-2014-6368, CVE-2014-6369, CVE-2014-6373, CVE-2014-6374, CVE-2014-6375, CVE-2014-6376, CVE-2014-8966, CVE-2014-6356, CVE-2014-6357, CVE-2014-6364, CVE-2014-6360, CVE-2014-6361, CVE-2014-6363, CVE-2014-6355

O CAIS recomenda que os administradores mantenham seus sistemas e aplicativos sempre atualizados, de acordo com as últimas versões e correções oferecidas pelos fabricantes.

Atenciosamente

CAIS/RNP


##########################################################

#############

# CENTRO DE ATENDIMENTO A INCIDENTES DE SEGURANCA (CAIS) #

# Rede Nacional de Ensino e Pesquisa (RNP)

#

#

#

# cais@cais.rnp.br

http://www.rnp.br/servicos/seguranca #

# Tel. 019-37873300 Fax. 019-37873301

#

# Chave PGP disponivel

http://www.rnp.br/cais/cais-pgp.key

##########################################################

#############