CAIS-Alerta: Resumo dos Boletins de Segurança Microsoft - Novembro/2014

[RNP, 17.11.2014]

A Microsoft publicou 15 boletins de segurança em 11 de novembro de 2014, que abordam, ao todo, 37 vulnerabilidades em produtos da empresa. A exploração dessas vulnerabilidades permite a execução remota de código, elevação de privilégio, desvio de recurso de segurança, divulgação de informações e negação de serviço.

Até o momento da publicação desse alerta, não foram divulgados códigos de exploração para as vulnerabilidades listadas.

SEVERIDADE

. Crítica

- MS14-064 - Vulnerabilidades no Windows OLE podem permitir a execução remota de código

- MS14-065 - Atualização de segurança cumulativa para o Internet Explorer

- MS14-066 - Vulnerabilidade no Schannel pode permitir execução remota de código

- MS14-067 - Vulnerabilidade no XML Core Services pode permitir a execução remota de código

. Importante

- MS14-069 - Vulnerabilidades no Microsoft Office podem permitir execução remota de código

- MS14-070 - Vulnerabilidade no TCP/IP pode permitir elevação de privilégio

- MS14-071 - Vulnerabilidade no serviço de áudio do Windows pode permitir a elevação de privilégio

- MS14-072 - Vulnerabilidade no.NET Framework pode permitir a elevação de privilégios

- MS14-073 - Vulnerabilidade no Microsoft SharePoint Foundation pode permitir elevação de privilégio

- MS14-074 - Vulnerabilidade no protocolo de área de trabalho remota pode permitir o desvio do recurso de segurança

- MS14-075 - Vulnerabilidades no Microsoft Exchange Server podem permitir elevação de privilégio

- MS14-076 - Vulnerabilidade no Internet Information Services (IIS) pode permitir o desvio do recurso de segurança

- MS14-077 - Vulnerabilidade nos serviços de Federação do Active Directory pode permitir a divulgação de informações

. Moderada

- MS14-078 - Vulnerabilidade no IME (japonês) pode permitir a elevação de privilégio

- MS14-079 - Vulnerabilidade no Driver de modo Kernel pode permitir negação de serviço

. 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/en-us/download/default.aspx

MAIS INFORMAÇÕES

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

https://technet.microsoft.com/pt-BR/library/security/ms14-nov.aspx

. 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-2014-6332, CVE-2014-6352, CVE-2014-4143, CVE-2014-6323, CVE-2014-6337,

CVE-2014-6339, CVE-2014-6340, CVE-2014-6341, CVE-2014-6342, CVE-2014-6343,

CVE-2014-6344, CVE-2014-6345, CVE-2014-6346, CVE-2014-6347, CVE-2014-6348,

CVE-2014-6349, CVE-2014-6350, CVE-2014-6351, CVE-2014-6353, CVE-2014-6321,

CVE-2014-4118, CVE-2014-6333, CVE-2014-6334, CVE-2014-6335, CVE-2014-4076,

CVE-2014-6322, CVE-2014-4149, CVE-2014-4116, CVE-2014-6318, CVE-2014-6319,

CVE-2014-6325, CVE-2014-6326, CVE-2014-6336, CVE-2014-4078, CVE-2014-6331,

CVE-2014-4077, CVE-2014-6317

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