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

Microsoft Security Bulletin Summary for January 2014

[RNP, 16.01.2014-, revisão 01]

A Microsoft publicou quatro (4) boletins de segurança em 14 de janeiro de 2014 que abordam ao todo seis (6) vulnerabilidades em produtos da empresa. A exploração dessas vulnerabilidades permite execução remota de código, elevação de privilégio e negação de serviço.

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

Severidade

- **Crítica**
- **Nenhum boletim**
- **Importante**
- **- MS14-001 - As vulnerabilidades no Microsoft Word e Office Web Apps podem permitir a execução remota de código**
- **- MS14-002 - Vulnerabilidade no kernel do Windows pode permitir a elevação de privilégio**
- **- MS14-003 - Vulnerabilidade nos drivers do modo do kernel do Windows pode permitir a elevação de privilégio**
- **- MS14-004 - A vulnerabilidade no Microsoft Dynamics AX pode permitir negação de serviço**
- **Moderada**
- **Nenhum boletim**

- **Baixa**
- **Nenhum boletim**

O sistema de classificação de severidade das vulnerabilidades adotado pelo CAIS nesse 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
- Microsoft Download Center

Mais informações

- Resumo do Boletim de Segurança da Microsoft de dezembro de 2013 (em inglês)
- Microsoft TechCenter de Segurança
- Microsoft Security Response Center - MSRC
- Microsoft Security Research & Defense - MSRD
- Central de Proteção e Segurança Microsoft

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

CVE-2014-0258, CVE-2014-0259, CVE-2014-0260, CVE-2013-5065, CVE-2014-0262, CVE-2014-0261

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 formato RSS/RDF e no Twitter:
http://www.rnp.br/cais/alertas/rss.xml
Siga @caisrnp.

CENTRO DE ATENDIMENTO A INCIDENTES DE SEGURANCA (CAIS)

Rede Nacional de Ensino e Pesquisa (RNP)

cais@cais.rnp.br

http://www.cais.rnp.br

Tel. 019-3787-3300 Fax. 019-3787-3301

Chave PGP disponível: http://www.rnp.br/cais/cais-pgp.key