CAIS-Alerta: Resumo dos Boletins de Segurança Microsoft - Janeiro/2013

Microsoft Security Bulletin Summary for January 2013

[RNP, 18.01.2013-, revisão 01]

A Microsoft publicou 7 boletins de segurança em 08 de janeiro de 2013 que abordam, ao todo, 11 vulnerabilidades em produtos da empresa. A exploração destas vulnerabilidades permitem execução remota de código, elevação de privilégios, negação de serviços, entre outros.

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

Severidade

- **Crítica**
    - **MS13-001 - Vulnerabilidade nos componentes do Spooler de impressão do Windows pode permitir execução remota de código.**
    - **MS13-002 - Vulnerabilidades no Microsoft XML Core Services podem permitir a execução remota de código**
- **Importante**
    - **MS13-003 - Vulnerabilidades no System Center Operations Manager podem permitir a elevação de privilégio.**
    - **MS13-004 - Vulnerabilidades no .NET Framework podem permitir elevação de privilégio.**
    - **MS13-005 - Vulnerabilidade no driver do modo do kernel do Windows pode permitir a elevação de privilégio.**
    - **MS13-006 - Vulnerabilidade no Microsoft Windows pode permitir burlar recurso de segurança.**
    - **MS13-007 - Vulnerabilidade no Protocolo de Dados Abertos (OData) pode permitir a realização de ataques de negação de serviço.**
- **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
- Microsoft Download Center

Mais informações

- Resumo do Boletim de Segurança da Microsoft de janeiro 2013
- 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-2013-0011, CVE-2013-0006, CVE-2013-0007, CVE-2013-0009, CVE-2013-0001, CVE-2013-0002, CVE-2013-0003, CVE-2013-0004, CVE-2013-0008, CVE-2013-0013, CVE-2013-0005

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