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

Alertas, vulnerabilidades e incidentes de segurança

[RNP, 13.03.2013-, revisão 01]

A Microsoft publicou 7 (sete) boletins de segurança em 12 de março de 2013 que abordam, ao todo, 20 vulnerabilidades em produtos da empresa. A exploração dessas vulnerabilidades permite a execução remota de código, elevação de privilégios, vazamento de informações, entre outros. Até o momento da publicação, existe a provável exploração de uma ou mais vulnerabilidades contidas no boletim MS13-021.

Severidade

- **Crítica**
    - **MS13-021 - Atualizações de segurança cumulativas para o Internet Explorer**
    - **MS13-022 - Vulnerabilidades no Microsoft Silverlight podem permitir a execução remota de código**
    - **MS13-023 - Vulnerabilidades no visualizador Microsoft Visio 2010 podem permitir a execução remota de código**
    - **MS13-024 - Vulnerabilidades no Microsoft SharePoint podem permitir elevação de privilégio**
- **Importante**
    - **MS13-025 - Vulnerabilidades no Microsoft OneNote podem permitir vazamento de informações**
    - **MS13-026 - Vulnerabilidades no Microsoft Office Outlook para usuários Mac podem permitir vazamento de informações**
    - **MS13-027 - Vulnerabilidade no driver do modo do kernel do Windows pode permitir a elevação de privilégio**
- **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 Março 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-2013-0087, CVE-2013-0088, CVE-2013-0089, CVE-2013-0090, CVE-2013-0091, CVE-2013-0092, CVE-2013-0093, CVE-2013-0094, CVE-2013-1288, CVE-2013-0074, CVE-2013-0079, CVE-2013-0080, CVE-2013-0083, CVE-2013-0084, CVE-2013-0085, CVE-2013-0086, CVE-2013-0095, CVE-2013-1285, CVE-2013-1286, CVE-2013-1287

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