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

Alertas, vulnerabilidades e incidentes de segurança

[RNP, 12.06.2013-, revisão 01]

A Microsoft publicou 5 boletins de segurança em 11 de junho de 2013 que abordam, ao todo, 22 vulnerabilidades em produtos da empresa. A exploração destas vulnerabilidades permite a execução remota de código, negação de serviço, elevação de privilégio, entre outros. Até o momento da publicação deste alerta, não foram divulgados códigos de exploração para as vulnerabilidades listadas.

Severidade

- **Crítica**
    - **MS13-047 - Atualização de segurança cumulativa para o Internet Explorer**
- **Importante**
    - **MS13-048 - Vulnerabilidades no Kernel do Windows podem permitir a divulgação indevida de informações**
    - **MS13-049 - Vulnerabilidade no Kernel-Mode Driver pode permitir a negação de serviço**
    - **MS13-050 - Vulnerabilidades nos componentes do Windows Print Spooler podem permitir elevação de privilégio**
    - **MS13-051 - Vulnerabilidade no Microsoft Office pode permitir a execução remota de código**
- **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 críticas e importantes. 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 junho 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-2013-3110, CVE-2013-3111, CVE-2013-3112, CVE-2013-3113, CVE-2013-3114, CVE-2013-3116, CVE-2013-3117, CVE-2013-3118, CVE-2013-3119, CVE-2013-3120, CVE-2013-3121, CVE-2013-3122, CVE-2013-3123, CVE-2013-3124, CVE-2013-3125, CVE-2013-3139, CVE-2013-3141, CVE-2013-3142, CVE-2013-3136, CVE-2013-3138, CVE-2013-1339, CVE-2013-1331

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