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

Alertas, vulnerabilidades e incidentes de segurança

[RNP, 16.04.2013-, revisão 01]

A Microsoft publicou 9 (nove) boletins de segurança em 9 de abril de 2013 que abordam ao todo 12 vulnerabilidades em produtos da empresa. A exploração dessas vulnerabilidades permite 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**
    - **MS13-028 - Atualização de segurança cumulativa para o Internet Explorer**
    - **MS13-029 - Vulnerabilidade no Remote Desktop Client pode permitir a execução remota de código**
- **Importante**
    - **MS13-030 - Vulnerabilidade no SharePoint pode permitir a divulgação de informações**
    - **MS13-031 - Vulnerabilidades no kernel do Windows podem permitir elevação de privilégio**
    - **MS13-032 - Vulnerabilidade no Active Directory pode permitir negação de serviço**
    - **MS13-033 - Vulnerabilidade no Windows Client / Server Runtime Subsystem (CSRSS) pode permitir elevação de privilégio**
    - **MS13-034 - Vulnerabilidade no Microsoft Antimalware Client pode permitir a elevação de privilégio**
    - **MS13-035 - Vulnerabilidade no componente de limpeza de HTML pode permitir elevação de privilégio**
    - **MS13-036 - Vulnerabilidades no driver no modo kernel 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 apliquem, 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 abril 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-2013-1303, CVE-2013-1304, CVE-2013-1296, CVE-2013-1290, CVE-2013-1284, CVE-2013-1282, CVE-2013-1295, CVE-2013-0078, CVE-2013-1289, CVE-2013-1283, CVE-2013-1292

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