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

Alertas, vulnerabilidades e incidentes de segurança

[RNP, 25.02.2013-, revisão 01]

A Microsoft publicou 12 boletins de segurança em 08 de janeiro de 2013, que abordam ao todo 53 vulnerabilidades em produtos da empresa. A exploração dessas vulnerabilidades permite execução remota de código, elevação de privilégios, negação de serviços, entre outros.

Severidade

- **Crítica**
    - **MS13-009 - Atualização de segurança cumulativa para o Internet Explorer**
    - **MS13-010 - Vulnerabilidade no Vector Markup Language pode permitir a execução remota de código**
    - **MS13-011 - Vulnerabilidade na descompactação de mídia pode permitir a execução remota de código**
    - **MS13-012 - Vulnerabilidades no Microsoft Exchange Server podem permitir a execução remota de código**
    - **MS13-020 - Vulnerabilidade na automação OLE pode permitir a execução remota de código**
- **Importante**
    - **MS13-013 - Vulnerabilidades na análise FAST Search**
    - **MS13-014 - Vulnerabilidade no NFS Server pode permitir a negação de serviço**
    - **MS13-015 - Vulnerabilidade no .NET Framework pode permitir a elevação de privilégio**
    - **MS13-016 - Vulnerabilidades no driver do modo do kernel do Windows pode permitir a elevação de privilégio**
    - **MS13-017 - Vulnerabilidades no kernel do Windows podem permitir a elevação de privilégio**
    - **MS13-018 - Vulnerabilidade no TCP/IP pode permitir negação de serviço**
    - **MS13-019 - Vulnerabilidade no Windows Client/Server Runtime Subsystem (CSRSS) pode permitir elevação de privilégio**
- **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 fevereiro 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-2013-0015, CVE-2013-0018, CVE-2013-0019, CVE-2013-0020, CVE-2013-0021, CVE-2013-0022, CVE-2013-0023, CVE-2013-0024, CVE-2013-0025, CVE-2013-0026, CVE-2013-0027, CVE-2013-0028, CVE-2013-0029, CVE-2013-0030,

CVE-2013-0077, CVE-2013-1281, CVE-2013-0073, CVE-2013-1248, CVE-2013-1249, CVE-2013-1250, CVE- 2013-1251, CVE-2013-1252, CVE-2013-1253, CVE-2013-1254, CVE-2013-1255, CVE-2013-1256, CVE-2013-1257, CVE-2013-1258, CVE-2013-1259, CVE-2013-1260, CVE-2013-1261, CVE-2013-1262, CVE-2013-1263, CVE-2013-1264, CVE-2013-1265, CVE-2013-1266, CVE-2013-1267, CVE-2013-1268, CVE- 2013-1269, CVE-2013-1270, CVE-2013-1271, CVE-2013-1272, CVE-2013-1273, CVE-2013-1274, CVE-2013-1275, CVE-2013-1276, CVE-2013-1277, CVE-2013-1278, CVE-2013- 1279, CVE-2013-1280, CVE-2013-0075, CVE-2013-0076, CVE-2013-1313

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