CAIS-Alerta: Resumo dos Boletins de Segurança Microsoft - Dezembro/2012

Microsoft Security Bulletin Summary for December 2012

[RNP, 13.12.2012-, revisão 01]

A Microsoft publicou 7 boletins de segurança em 11 de dezembro que abordam ao todo 13 vulnerabilidades em produtos da empresa. A exploração destas vulnerabilidades permitem execução remota de código e transposição de recurso de segurança.

Até o momento da publicação deste alerta há exploração ativa de 1 vulnerabilidade (MS12-080).

Severidade

- **Crítica**
    - **MS12-077 - Atualização de segurança cumulativa para o Internet Explorer**
    - **MS12-078 - Vulnerabilidades em drivers do modo do kernel do Windows podem permitir a execução remota de código**
    - **MS12-079 - Vulnerabilidade no Microsoft Word pode permitir a execução remota de código**
    - **MS12-080 - Vulnerabilidades no servidor Microsoft Exchange podem permitir a execução remota de código**
    - **MS12-081 - Vulnerabilidade no componente Windows File Handling pode permitir a execução remota de código**
- **Importante**
    - **MS12-082 - Vulnerabilidade no DirectPlay podem permitir a execução remota de código**
    - **MS12-083 - Vulnerabilidade no componente IP-HTTPS pode permitir transposição de recurso de segurança**
- **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
- Windows Server Update Services

Mais informações

- Resumo do Boletim de Segurança da Microsoft de dezembro de 2012
- Microsoft TechCenter de Segurança
- Microsoft Security Response Center - MSRC
- Microsoft Security Research & Defense - MSRD
- Segurança Microsoft

Identificador CVE (http://cve.mitre.org):

CVE-2012-1537, CVE-2012-2539, CVE-2012-2545, CVE-2012-2549, CVE-2012-2556, CVE-2012-3214, CVE-2012-3217, CVE-2012-4774, CVE-2012-4781, CVE-2012-4782, CVE-2012-4786, CVE-2012-4787, CVE-2012-4791

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