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

Microsoft Security Bulletin Summary for October 2012

[RNP, 10.10.2012-, revisão 01]

A Microsoft publicou 7 boletins de segurança em 9 de outubro que abordam ao todo 8 vulnerabilidades em produtos da empresa. A exploração destas vulnerabilidades permitem execução remota de código, negação de serviço e elevação de privilégio.

Até o momento da publicação deste alerta, há exploração ativa de duas vulnerabilidades (MS12-066 e MS12-067).

Severidade

- **Crítica**
    - **MS12-064 - Vulnerabilidades no Microsoft Word podem permitir a execução remota de código**
- **Importante**
    - **MS12-065 - Vulnerabilidades no Microsoft Works podem permitir a execução remota de código**
    - **MS12-066 - Vulnerabilidade no componente de sanitização de HTML pode permitir a elevação de privilégioMS12-062 - Vulnerabilidade no Microsoft System Center Configuration Manager pode permitir elevação de privilégio**
    - **MS12-067 - Vulnerabilidades no FAST Search Server 2010 para SharePoint podem permitir a execução remota de código**
    - **MS12-068 - Vulnerabilidade no kernel do Windows pode permitir a elevação de privilégio**
    - **MS12-069 - Vulnerabilidade no Kerberos pode permitir negação de serviço**
    - **MS12-070 - Vulnerabilidade no SQL Server pode permitir a 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 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 outubro 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-2012-0182, CVE-2012-0182, CVE-2012-1766, CVE-2012-1767, CVE-2012-1768, CVE-2012-1769, CVE-2012-1770, CVE-2012-1771, CVE-2012-1772, CVE-2012-1773, CVE-2012-2520, CVE-2012-2528, CVE-2012-2528, CVE-2012-2529, CVE-2012-2550, CVE-2012-2551, CVE-2012-3106, CVE-2012-3107, CVE-2012-3108, CVE-2012-3109, CVE-2012-3110

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