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

Microsoft Security Bulletin Summary for December 2012

[RNP, 17.01.2012-, revisão 01]

A Microsoft publicou 7 boletins de segurança em 11 de janeiro que abordam ao todo 8 vulnerabilidades permitem execução remota de código, desvio de recurso de segurança, elevação de privilégio e divulgação não autorizada de informação.

Severidade

- **Crítica**
    - **MS12-004 - Vulnerabilidades no Windows Media podem permitir a execução remota de código.**
- **Importante**
    - **MS12-001 - Vulnerabilidade no kernel do Windows pode permitir o desvio do recurso de segurança.**
    - **MS12-002 - Vulnerabilidade no Windows Object Packager pode permitir a execução remota de código.**
    - **MS12-003 - Vulnerabilidade no Windows Client/Server Run-time Subsystem pode permitir elevação de privilégio.**
    - **MS12-005 - Vulnerabilidade no Microsoft Windows pode permitir a execução remota de código.**
    - **MS12-006 - Vulnerabilidade no SSL/TLS pode permitir divulgação não autorizada de informações.**
    - **MS12-007 - Vulnerabilidade na AntiXSS pode permitir a divulgação não autorizada de informações.**
- **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 pode 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 janeiro 2012
- Microsoft TechCenter de Segurança
- Microsoft Security Response Center - MSRC
- Microsoft Security Research & Defense - MSRD
- Segurança Microsoft
- MS12-001 - Vulnerabilidade no kernel do Windows pode permitir o desvio do recurso de segurança
- MS12-002 - Vulnerabilidade no Windows Object Packager pode permitir a execução remota de código
- MS12-003 - Vulnerabilidade no Windows Client/Server Run-time Subsystem pode permitir elevação de privilégio
- MS12-004 - Vulnerabilidades no Windows Media podem permitir a execução remota de código
- MS12-005 - Vulnerabilidade no Microsoft Windows pode permitir a execução remota de código
- MS12-006 - Vulnerabilidade no SSL/TLS pode permitir divulgação não autorizada de informações
- MS12-007 - Vulnerabilidade na AntiXSS pode permitir a divulgação não autorizada de informações

Identificador CVE (http://cve.mitre.org):
CVE-2011-3389, CVE-2012-0001, CVE-2012-0009, CVE-2012-0005, CVE-2012-0003, CVE-2012-0004, CVE-2012-0013, CVE-2012-0007

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.