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

Microsoft Security Bulletin Summary for May 2012

[RNP, 15.05.2012-, revisão 01]

A Microsoft publicou 7 boletins de segurança em 8 de maio que abordam ao todo 22 vulnerabilidades em produtos da empresa. A exploração destas vulnerabilidades permitem execução remota de código e elevação de privilégio.

Severidade

- **Crítica**
    - **MS12-029 - Vulnerabilidade no Microsoft Word pode permitir a execução remota de código**
    - **MS12-034 - Atualização de segurança combinada para Microsoft Office, Windows, .NET Framework e Silverlight.**
    - **MS12-035 - Vulnerabilidade no .NET Framework pode permitir execução remota de código.**
- **Importante**
    - **MS12-030 - Vulnerabilidades no Microsoft Office podem permitir a execução remota de código.**
    - **MS12-031 - Vulnerabilidade no Microsoft Visio Viewer 2010 pode permitir a execução remota de código.**
    - **MS12-032 - Vulnerabilidade no TCP/IP pode permitir a elevação de privilégio.**
    - **MS12-033 - Vulnerabilidade no Windows Partition pode permitir a elevação de privilégio.**
- **Moderada**
- **Nenhum boletim**
- **Baixa**

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 maio 2012
- Microsoft TechCenter de Segurança
- Microsoft Security Response Center - MSRC
- Microsoft Security Research & Defense - MSRD
- Segurança Microsoft
- MS12-029 - Vulnerabilidade no Microsoft Word pode permitir a execução remota de código
- MS12-034 - Atualização de segurança combinada para Microsoft Office, Windows, .NET Framework e Silverlight
- MS12-035 - Vulnerabilidade no .NET Framework pode permitir execução remota de código
- MS12-030 - Vulnerabilidades no Microsoft Office podem permitir a execução remota de código
- MS12-031 - Vulnerabilidade no Microsoft Visio Viewer 2010 pode permitir a execução remota de código
- MS12-032 - Vulnerabilidade no TCP/IP pode permitir a elevação de privilégio
- MS12-033 - Vulnerabilidade no Windows Partition pode permitir a elevação de privilégio

Identificador CVE (http://cve.mitre.org):
CVE-2012-0183, CVE-2012-0141, CVE-2012-0142,

CVE-2012-0143, CVE-2012-0184, CVE-2012-0185, CVE-2012-1847, CVE-2012-0018, CVE-2012-0174, CVE-2012-0179, CVE-2012-0178, CVE-2012-3402, CVE-2012-0159, CVE-2012-0162, CVE-2012-0165, CVE-2012-0167, CVE-2012-0176, CVE-2012-0180, CVE-2012-0181, CVE-2012-1848, CVE-2012-0161, CVE-2012-0161

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.