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

Microsoft Security Bulletin Summary for July 2012

[RNP, 11.07.2012-, revisão 01]

A Microsoft publicou 9 boletins de segurança em 10 de julho que abordam ao todo 16 vulnerabilidades em produtos da empresa. A exploração destas vulnerabilidades permitem execução remota de código, elevação de privilégio e vazamento de informações.

Até o momento da publicação deste alerta não há exploração ativa das vulnerabilidades, porém algumas são publicamente conhecidas (MS12-043, MS12-046, MS12-047, MS12-050 e MS12-051) e há uma prova de conceito (PoC) disponível para exploração da MS12-049.

**Severidade**

- **Crítica**
    - **MS12-043 - Vulnerabilidade no Microsoft XML Core Services pode permitir execução remota de código**
    - **MS12-044 - Atualização cumulativa de segurança para Microsoft Internet Explorer**
    - **MS12-045 - Vulnerabilidade no Microsoft Data Access Components pode permitir execução remota de código**
- **Importante**
    - **MS12-046 - Vulnerabilidade no Visual Basic para aplicações pode permitir execução remota de código.**
    - **MS12-047 - Vulnerabilidades em drivers kernel-mode do Windows podem permitir elevação de privilégio**
    - **MS12-048 - Vulnerabilidade no Windows shell pode permitir execução remota de código**
    - **MS12-049 - Vulnerabilidade no TLS pode permitir vazamento de informações**
    - **MS12-050 - Vulnerabilidades no SharePoint pode permitir elevação de privilégio**
    - **MS12-051 - Vulnerabilidade no Microsoft Office para Mac pode permitir 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 julho 2012
- Microsoft TechCenter de Segurança
- Microsoft Security Response Center - MSRC
- Microsoft Security Research & Defense - MSRD
- Segurança Microsoft
- MS12-043 - Vulnerabilidade no Microsoft XML Core Services pode permitir execução remota de código
- MS12-044 - Atualização cumulativa de segurança para Microsoft Internet Explorer
- MS12-045 - Vulnerabilidade no Microsoft Data Access Components pode permitir execução remota de código
- MS12-046 - Vulnerabilidade no Visual Basic para aplicações pode permitir execução remota de código
- MS12-047 - Vulnerabilidades em drivers kernel-mode do Windows podem permitir elevação de privilégio
- MS12-048 - Vulnerabilidade no Windows shell pode permitir execução remota de código

- MS12-049 - Vulnerabilidade no TLS pode permitir vazamento de informações
- MS12-050 - Vulnerabilidades no SharePoint pode permitir elevação de privilégio
- MS12-051 - Vulnerabilidade no Microsoft Office para Mac pode permitir elevação de privilégio

Identificador CVE (http://cve.mitre.org):
CVE-2012-0175, CVE-2012-1522, CVE-2012-1524, CVE-2012-1854, CVE-2012-1858, CVE-2012-1859, CVE-2012-1860, CVE-2012-1861, CVE-2012-1863, CVE-2012-1870, CVE-2012-1889, CVE-2012-1890, CVE-2012-1891, CVE-2012-1893, CVE-2012-1894

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