# CAIS-Alerta: Resumo dos Boletins de Segurança Microsoft - Maio/2014

Microsoft Security Bulletin Summary for May 2014

[RNP, 16.05.2014, revisão 01]

A Microsoft publicou nove (9) boletins de segurança em 13 de maio de 2014, que abordam ao todo 14 vulnerabilidades em produtos da empresa. A exploração dessas vulnerabilidades permite a execução remota de código, a elevação de privilégio, a negação de serviço e o desvio de recurso de segurança.

Até o momento da publicação desse alerta, não foram divulgados códigos de exploração para as vulnerabilidades listadas.

**Severidade**

- **Crítica**
    - **MS14-021 - Atualização de segurança para o Internet Explorer**
    - **MS14-029 - Atualização de segurança para o Internet Explorer**
    - **MS14-022 - Vulnerabilidades no Microsoft SharePoint Server podem permitir a execução remota de código**
- **Importante**
    - **MS14-023 - Vulnerabilidades no Microsoft Office podem permitir a execução remota de código**
    - **MS14-025 - Vulnerabilidade nas preferências da Diretiva de Grupo pode permitir a elevação de privilégio**
    - **MS14-026 - Vulnerabilidade no .NET Framework pode permitir elevação de privilégio**
    - **MS14-027 - Vulnerabilidade no Windows Shell Handler pode permitir a elevação de privilégio**
    - **MS14-028 - Vulnerabilidade no iSCSI pode permitir a negação de serviço**
    - **MS14-024 - Vulnerabilidade em um controle comum da Microsoft pode permitir desvio do recurso de segurança**
- **Moderada**
- **Nenhum boletim**

- **Baixa**
- **Nenhum boletim**

O sistema de classificação de severidade das vulnerabilidades adotado pelo CAIS nesse 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 de 2014
- Microsoft TechCenter de Segurança
- Microsoft Security Response Center - MSRC
- Microsoft Security Research & Defense - MSRD
- Central de Proteção e Segurança Microsoft

Identificador CVE (http://cve.mitre.org):
CVE-2014-1776, CVE-2014-0251, CVE-2014-1754, CVE-2014-1813, CVE-2014-1756, CVE-2014-1808, CVE-2014-1809, CVE-2014-1812, CVE-2014-1806, CVE-2014-1807, CVE-2014-0255, CVE-2014-0256, CVE-2014-0310, CVE-2014-1815

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.