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

Microsoft Security Bulletin Summary for February 2014

[RNP, 13.02.2014-, revisão 01]

A Microsoft publicou sete (7) boletins de segurança em 11 de fevereiro de 2014, que abordam ao todo 32 vulnerabilidades em produtos da empresa. A exploração dessas vulnerabilidades permitem execução remota de código, elevação de privilégio, divulgação não autorizada de informação e negação de serviço. Até o momento da publicação desse alerta, não foram divulgados códigos de exploração para as vulnerabilidades listadas.

Severidade

- **Crítica**
    - **MS14-010 – Atualização de segurança cumulativa para o Internet Explorer**
    - **MS14-011 - Vulnerabilidade no mecanismo de script VBScript pode permitir execução remota de código**
    - **MS14-007 - Vulnerabilidade no Direct2D pode permitir a execução remota de código**
    - **MS14-008 - Vulnerabilidade no Microsoft Forefront Protection for Exchange pode permitir a execução remota de código**
- **Importante**
    - **MS14-009 - Vulnerabilidades no .NET Framework podem permitir a elevação de privilégio**
    - **MS14-005 - Vulnerabilidade no Microsoft XML Core Services pode permitir a divulgação de informações**
    - **MS14-006 - Vulnerabilidade no IPv6 pode permitir a negação de serviço**
- **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 fevereiro 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-2014-0266, CVE-2014-0254, CVE-2014-0263, CVE-2014-0294, CVE-2014-0253, CVE-2014-0257, CVE-2014-0295, CVE-2014-0267, CVE-2014-0268, CVE-2014-0269, CVE-2014-0270, CVE-2014-0271, CVE-2014-0272, CVE-2014-0273, CVE-2014-0274, CVE-2014-0275, CVE-2014-0276, CVE-2014-0277, CVE-2014-0278, CVE-2014-0279, CVE-2014-0280, CVE-2014-0281, CVE-2014-0283, CVE-2014-0284, CVE-2014-0285, CVE-2014-0286, CVE-2014-0287, CVE-2014-0288, CVE-2014-0289, CVE-2014-0290, CVE-2014-0293, CVE-2014-0271

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.