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

Microsoft Security Bulletin Summary for March 2014

[RNP, 13.03.2014-, revisão 01]

A Microsoft publicou cinco (5) boletins de segurança em 11 de março de 2014, que abordam ao todo 23 vulnerabilidades em produtos da empresa. A exploração dessas vulnerabilidades permite execução remota de código, elevação de privilégio e desvio de recurso de segurança.Até o momento da publicação desse alerta, não foram divulgados códigos de exploração para as vulnerabilidades listadas.

Severidade

- **Crítica**
    - **MS14-012 - Atualização de segurança cumulativa para o Internet**
    - **MS14-013 - Vulnerabilidade no Microsoft DirectShow pode permitir a execução remota de código**
- **Importante**
    - **MS14-015 - Vulnerabilidades no driver do modo do kernel do Windows podem permitir a elevação de privilégio**
    - **MS14-016 - Vulnerabilidade no protocolo Remoto do Gerente de Conta de Segurança (SAMR) pode permitir o desvio do recurso de segurança**
    - **MS14-014 - Vulnerabilidade no Silverlight pode permitir o desvio do recurso de segurança**
- **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 março 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-2014-0297, CVE-2014-0298, CVE-2014-0299, CVE-2014-0302, CVE-2014-0303, CVE-2014-0304, CVE-2014-0305, CVE-2014-0306, CVE-2014-0307, CVE-2014-0308, CVE-2014-0309, CVE-2014-0311, CVE-2014-0312, CVE-2014-0313, CVE-2014-0314, CVE-2014-0321, CVE-2014-0322, CVE-2014-0324, CVE-2014-0301, CVE-2014-0319, CVE-2014-0300, CVE-2014-0323, CVE-2014-0317

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.