CAIS-Alerta: Resumo dos Boletins de Segurança Microsoft - Julho/2013

Alertas, vulnerabilidades e incidentes de segurança

[RNP, 11.07.2013-, revisão 01]

A Microsoft publicou 7 boletins de segurança em 9 de julho de 2013 que abordam ao todo 35 vulnerabilidades em produtos da empresa. A exploração dessas vulnerabilidades permite execução remota de código e elevação de privilégio. Até o momento da publicação deste alerta, não foram divulgados códigos de exploração para as vulnerabilidades listadas.

Severidade

- **Crítica**
- **- MS13-052 - Vulnerabilidades no .NET Framework e Silverlight podem permitir a execução remota de código**
- **- MS13-053 - Vulnerabilidades nos drivers Kernel-Mode do Windows podem permitir a execução remota de código**
- **- MS13-054 - Vulnerabilidades no GDI+ podem permitir a execução remota de código**
- **- MS13-055 - Update de segurança cumulativa para Internet Explorer**
- **- MS13-056 - Vulnerabilidades no Microsoft DirectShow podem permitir a execução remota de código**
- **- MS13-057 - Vulnerabilidades no Windows Media Format Runtime podem permitir a execução remota de código**
- **Importante**
- **- MS13-058 - Vulnerabilidades no Windows Defender podem permitir a execução remota de código**
- **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 possa 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
- Microsoft Download Center

Mais informações

- Resumo do Boletim de Segurança da Microsoft de julho de 2013 (em inglês)
- 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-2013-3129, CVE-2013-3131, CVE-2013-3132, CVE-2013-3133, CVE-2013-3134, CVE-2013-3171, CVE-2013-3178, CVE-2013-1300, CVE-2013-1340, CVE-2013-1345, CVE-2013-3129, CVE-2013-3167, CVE-2013-3173, CVE-2013-3660, CVE-2013-3129, CVE-2013-3115, CVE-2013-3143, CVE-2013-3144, CVE-2013-3145, CVE-2013-3146, CVE-2013-3147, CVE-2013-3148, CVE-2013-3149, CVE-

2013-3150, CVE-2013-3151, CVE-2013-3152, CVE-2013-3153, CVE-2013-3161, CVE-2013-3162, CVE-2013-3163, CVE-2013-3164, CVE-2013-3166, CVE-2013-3174, CVE-2013-3127, CVE-2013-3154

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