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

Alertas, vulnerabilidades e incidentes de segurança

[RNP, 20.05.2013-, revisão 01]

A Microsoft publicou 10 boletins de segurança em 14 de maio de 2013 que abordam ao todo 33 vulnerabilidades em produtos da empresa. A exploração dessas vulnerabilidades permite execução remota de código, negação de serviço, divulgação não autorizada de informações, entre outros. Até o momento da publicação deste alerta, não foram divulgados códigos de exploração para as vulnerabilidades listadas.

Severidade

- **Crítica**
    - **MS13-037 - Atualização de segurança cumulativa para o Internet Explorer**
    - **MS13-038 - Atualização de segurança para o Internet Explorer**
- **Importante**
    - **MS13-039 - Vulnerabilidade no HTTP.sys pode permitir a negação de serviço**
    - **MS13-040 - Vulnerabilidades no .NET Framework podem permitir falsificação**
    - **MS13-041 - Vulnerabilidade no Lync pode permitir a execução remota de código**
    - **MS13-042 - Vulnerabilidades no Microsoft Publisher podem permitir a execução remota de código**
    - **MS13-043 - Vulnerabilidade no Microsoft Word pode permitir a execução remota de código**
    - **MS13-044 - Vulnerabilidade no Microsoft Visio pode permitir a divulgação de informações**
    - **MS13-045 - Vulnerabilidade no Windows Essentials pode permitir a divulgação não autorizada de informações**
    - **MS13-046 - Vulnerabilidades nos drivers do modo kernel podem permitir a elevação de privilégio**
- **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 maio 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-2013-0811, CVE-2013-1297, CVE-2013-1306, CVE-2013-1307, CVE-2013-1308, CVE-2013-1309, CVE-2013-1310, CVE-2013-1311, CVE-2013-1312, CVE-2013-1313, CVE-2013-2551, CVE-2013-1347, CVE-2013-1305, CVE-2013-1336, CVE-2013-1337, CVE-2013-1302, CVE-2013-1316, CVE-2013-1317, CVE-2013-1318, CVE-2013-1319, CVE- 2013-1320, CVE-2013-1321, CVE-2013-1322, CVE-2013-1323, CVE-2013-1327, CVE-2013-1328, CVE-2013-1329, CVE-2013-1335,

CVE-2013-1301, CVE-2013-0096, CVE-2013- 1332, CVE-2013-1333, CVE-2013-1334

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