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

Microsoft Security Bulletin Summary for December 2013

[RNP, 11.12.2013-, revisão 01]

A Microsoft publicou 11 boletins de segurança em 10 de dezembro de 2013 que abordam ao todo 24 vulnerabilidades em produtos da empresa. A exploração dessas vulnerabilidades permitem execução remota de código, elevação de privilégio, divulgação não autorizada de informação 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**
- **- MS13-096 - Vulnerabilidade no componente do Microsoft Graphics pode permitir a execução remota de código**
- **- MS13-097 - Atualização de segurança cumulativa para o Internet Explorer**
- **- MS13-098 - Vulnerabilidade no Windows pode permitir a execução remota de código**
- **- MS13-099 - A vulnerabilidade na Biblioteca de Objetos do Microsoft Scripting Runtime pode permitir a execução remota de código**
- **- MS13-105 - Vulnerabilidades no Microsoft Exchange Server podem permitir a execução remota de código**
- **Importante**
- **- MS13-100 - Vulnerabilidades no Microsoft SharePoint Server podem permitir a execução remota de código**
- **- MS13-101 - Vulnerabilidades nos drivers do modo kernel do Windows podem permitir a elevação de privilégio**

- **- MS13-102 - Vulnerabilidade no Cliente LRPC pode permitir a elevação de privilégio**
- **- MS13-103 - Vulnerabilidade no ASP.NET SignalR pode permitir a elevação de privilégio**
- **- MS13-104 - Vulnerabilidade no Microsoft Office pode permitir a divulgação de informações**
- **- MS13-106 - Vulnerabilidade em um componente compartilhado do Microsoft Office pode permitir desvio de 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 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 outubro 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-2013-3906, CVE-2013-5045, CVE-2013-5046, CVE-2013-5047, CVE-2013-5048, CVE-2013-5049, CVE-2013-5051, CVE-2013-5052, CVE-2013-3900, CVE-2013-5056, CVE-2013-5059, CVE-2013-3899, CVE-2013-3902, CVE-2013-3903, CVE-2013-3907, CVE-2013-5058, CVE-2013-3878, CVE-2013-5042, CVE-2013-5054, CVE-2013-1330, CVE-2013-5763, CVE-2013-5791, CVE-2013-5072, CVE-2013-5057

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