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

Microsoft Security Bulletin Summary for September 2013

[RNP, 19.09.2013-, revisão 01]

A Microsoft publicou 13 boletins de segurança em 10 de setembro de 2013 que abordam ao todo 53 vulnerabilidades em produtos da empresa. A exploração destas vulnerabilidades permitem execução remota de código, negação de serviço e elevação de privilégio dentre outras.

Até o momento da publicação deste alerta não foram divulgados códigos de exploração para as vulnerabilidades listadas.

Severidade

- **Crítica**
- **- MS13-067 - Vulnerabilidades no Microsoft SharePoint Server podem permitir a execução remota de código**
- **- MS13-068 - Vulnerabilidade no Microsoft Outlook pode permitir a execução remota de código**
- **- MS13-069 - Atualização de segurança cumulativa para o Internet Explorer**
- **- MS13-070 - Vulnerabilidade no OLE pode permitir a execução remota de código**
- **Importante**
- **- MS13-071 - Vulnerabilidade no arquivo de tema do Windows pode permitir execução remota de código**
- **- MS13-072 - Vulnerabilidades no Microsoft Office podem permitir a execução remota de código**
- **- MS13-073 - Vulnerabilidades no Microsoft Excel podem permitir a execução remota de código**

- **- MS13-074 - Vulnerabilidades no Microsoft Access podem permitir a execução remota de código**
- **- MS13-075 - Vulnerabilidade no Microsoft Office IME (chinês) pode permitir a elevação de privilégio**
- **- MS13-076 - Vulnerabilidades nos drivers do modo kernel podem permitir a elevação de privilégio**
- **- MS13-077 - Vulnerabilidade no Gerenciador de Controle de Serviços do Windows pode permitir a elevação de privilégio**
- **- MS13-078 - Vulnerabilidade no FrontPage pode permitir divulgação não autorizada de informações**
- **- MS13-079 - Vulnerabilidade no Active Directory 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 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 setembro 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-2013-0081, CVE-2013-1315, CVE-2013-1330, CVE-2013-3179, CVE-2013-3180, CVE-2013-3847, CVE-2013-3848, CVE-2013-3849, CVE-2013-3857, CVE-2013-3858, CVE-2013-3870, CVE-2013-3201, CVE-2013-3202, CVE-2013-3203, CVE-2013-3204, CVE-2013-3205, CVE-2013-3206, CVE-2013-3207, CVE-2013-3208, CVE-2013-3209, CVE-2013-3845, CVE-2013-3863, CVE-2013-0810, CVE-2013-3160, CVE-2013-3847, CVE-2013-3848, CVE-2013-3849, CVE-2013-3850, CVE-2013-3851, CVE-2013-3852, CVE-2013-3853, CVE-2013-3854, CVE-2013-3855, CVE-2013-3856, CVE-2013-3857, CVE-2013-3858, CVE-2013-1315, CVE-2013-3158, CVE-2013-3159, CVE-2013-3155, CVE-2013-3156, CVE-2013-3157, CVE-2013-3859, CVE-2013-1341, CVE-2013-1342, CVE-2013-1343, CVE-2013-1344, CVE-2013-3864, CVE-2013-3865, CVE-2013-3866, CVE-2013-3862, CVE-2013-3137, CVE-2013-3868

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