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

Microsoft Security Bulletin Summary for November 2013

[RNP, 14.11.2013-, revisão 01]

A Microsoft publicou 8 boletins de segurança em 12 de novembro de 2013 que abordam ao todo 19 vulnerabilidades em produtos da empresa. A exploração dessas vulnerabilidades permitem execução remota de código, negação de serviço e elevação de privilégio.

Até a divulgação deste alerta existem relatos de exploração das vulnerabilidades relacionadas ao boletim MS13-090. Para mais informações consultar o site: http://blogs.technet.com/b/msrc/archive/2013/11/11/activex-control-issue-being-addressed-in-update-tuesday.aspx

Severidade

- **Crítica**
- **- MS13-088 - Atualização de segurança cumulativa para o Internet Explorer**
- **- MS13-089 - Vulnerabilidade no Windows Graphics Device Interface pode permitir execução remota de código**
- **- MS13-090 - Atualização de segurança cumulativa de Kill Bits do ActiveX**
- **Importante**
- **- MS13-091 - Vulnerabilidades no Microsoft Office podem permitir a execução remota de código**
- **- MS13-092 - Vulnerabilidade no Hyper-V pode permitir elevação de privilégio**
- **- MS13-093 - Vulnerabilidade no Microsoft Ancillary Function Driver pode permitir a divulgação de informação**
- **- MS13-094 - Vulnerabilidade no Microsoft Outlook pode permitir a divulgação de informações**

- **- MS13-095 - Vulnerabilidade de assinatura digital pode permitir a negação de serviço**
- **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 novembro 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-2013-3871, CVE-2013-3908, CVE-2013-3909, CVE-2013-3910, CVE-2013-3911, CVE-2013-3912, CVE-2013-3914, CVE-2013-3915, CVE-2013-3916, CVE-2013-3917, CVE-2013-3940, CVE-2013-3918, CVE-2013-0082, CVE-2013-1324, CVE-2013-1325, CVE-2013-3898, CVE-2013-3887, CVE-2013-3905, CVE-2013-3869

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