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

Microsoft Security Bulletin Summary for October 2013

[RNP, 09.10.2013-, revisão 01]

A Microsoft publicou 8 boletins de segurança em 8 de outubro de 2013 que abordam ao todo 28 vulnerabilidades em produtos da empresa. A exploração dessas vulnerabilidades permite execução remota de código, negação de serviço e elevação de privilégio.

Até a divulgação desse alerta, existem relatos de exploração das vulnerabilidades relacionadas ao boletim MS13-080. Para mais informações, consultar o site http://blogs.technet.com/b/srd/archive/2013/10/08/ms13-080-addresses-two-vulnerabilities-under-limited-targeted-attacks.aspx (em inglês).

Severidade

- **Crítica**
- **- MS13-080 - Atualização de segurança cumulativa para o Internet Explorer**
- **- MS13-081 - Vulnerabilidades em drivers do modo do kernel do Windows podem permitir a execução remota de código**
- **- MS13-082 - Vulnerabilidades no .NET Framework podem permitir a execução remota de código**
- **- MS13-083 - Vulnerabilidade na biblioteca de controle comum do Windows permite a execução remota de código**
- **Importante**
- **- MS13-084 - Vulnerabilidades no Microsoft SharePoint Server podem permitir a execução remota de código**
- **- MS13-085 - Vulnerabilidades no Microsoft Excel podem permitir a execução remota de código**
- **- MS13-086 - Vulnerabilidades no Microsoft Word podem permitir a execução remota de código**

- **- MS13-087 - A vulnerabilidade no Silverlight pode permitir a divulgação não autorizada de informação**
- **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 críticas e importantes. 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-2013-3871, CVE-2013-3872, CVE-2013-3873, CVE-2013-3874, CVE-2013-3875, CVE-2013-3882, CVE-2013-3885, CVE-2013-3886, CVE-2013-3893, CVE-2013-3897, CVE-2013-3128, CVE-2013-3200, CVE-2013-3879, CVE-2013-3880, CVE-2013-3881, CVE-2013-3888, CVE-2013-3894, CVE-2013-3128, CVE-2013-3860, CVE-2013-3861, CVE-2013-3195, CVE-2013-3889, CVE-2013-3895, CVE-2013-3889, CVE-2013-3890, CVE-2013-3891, CVE-2013-3892, CVE-2013-3896

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