

## CAIS-Alerta: Resumo dos Boletins de Segurança Microsoft - Outubro/2014

### Microsoft Security Bulletin Summary for October 2014

[RNP, 17.10.2014]

A Microsoft publicou oito (8) boletins de segurança em 14 de outubro de 2014, que abordam ao todo 24 vulnerabilidades em produtos da empresa. A exploração dessas vulnerabilidades permite execução remota de código, elevação de privilégio 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

- MS14-056 - Atualização de segurança cumulativa para o Internet Explorer
- MS14-057 - Vulnerabilidades no .NET Framework podem permitir a execução remota de código
- MS14-058 - Vulnerabilidade no driver do modo kernel podem permitir a execução remota de código

##### . Importante

- MS14-059 - Vulnerabilidade no ASP.NET MVC pode permitir o desvio de recurso de segurança
- MS14-060 - Vulnerabilidade no Windows OLE pode permitir a execução remota de código
- MS14-061 - A vulnerabilidade no Microsoft Word e Office Web Apps pode permitir a execução remota de código
- MS14-062 - Vulnerabilidade no serviço de Enfileiramento de Mensagens pode permitir a elevação de privilégio
- MS14-063 - Vulnerabilidade no driver da partição do disco FAT32 pode 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

<https://www.update.microsoft.com/microsoftupdate/>

. Microsoft Download Center

<http://www.microsoft.com/en-us/download/default.aspx>

### **MAIS INFORMAÇÕES**

. Resumo do Boletim de Segurança da Microsoft de outubro de 2014

<https://technet.microsoft.com/pt-BR/library/security/ms14-oct.aspx>

. Microsoft TechCenter de Segurança

<http://technet.microsoft.com/pt-br/security/>

. Microsoft Security Response Center - MSRC

<http://www.microsoft.com/security/msrc/>

. Microsoft Security Research & Defense - MSRD

<http://blogs.technet.com/srd/>

. Central de Proteção e Segurança Microsoft

<http://www.microsoft.com/brasil/security/>

Identificador CVE (<http://cve.mitre.org> <<http://cve.mitre.org/>>):

CVE-2014-4123, CVE-2014-4124, CVE-2014-4126, CVE-2014-4127, CVE-2014-4128,  
CVE-2014-4129, CVE-2014-4130, CVE-2014-4132, CVE-2014-4133, CVE-2014-4134,  
CVE-2014-4137, CVE-2014-4138, CVE-2014-4140, CVE-2014-4141, CVE-2014-4073,  
CVE-2014-4121, CVE-2014-4122, CVE-2014-4113, CVE-2014-4148, CVE-2014-4075,  
CVE-2014-4114, CVE-2014-4117, CVE-2014-4971, CVE-2014-4115

O CAIS recomenda que os administradores mantenham seus sistemas e aplicativos sempre atualizados, de acordo com as últimas versões e correções oferecidas pelos fabricantes.