

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

Microsoft Security Bulletin Summary for September 2014

[RNP, 15.09.2014]

A Microsoft publicou quatro (4) boletins de segurança em 9 de setembro de 2014, que abordam ao todo 42 vulnerabilidades em produtos da empresa. A exploração dessas vulnerabilidades permite a execução remota de código, elevação de privilégio e negação de serviço.

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

SEVERIDADE

. Crítica

- MS14-052 - Atualização de segurança cumulativa para Internet Explorer

. Importante

- MS14-053 - Vulnerabilidade no .NET Framework pode permitir elevação de privilégio

- MS14-054 - Vulnerabilidade no Agendador de Tarefas do Windows pode permitir a elevação de privilégio

- MS14-055 - Vulnerabilidades no Microsoft Lync Server Could podem 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

<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 setembro de 2014

<https://technet.microsoft.com/library/security/ms14-sep.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-2013-7331, CVE-2014-2799, CVE-2014-4059, CVE-2014-4065, CVE-2014-4079,
CVE-2014-4080, CVE-2014-4081, CVE-2014-4082, CVE-2014-4083, CVE-2014-4084,
CVE-2014-4085, CVE-2014-4086, CVE-2014-4087, CVE-2014-4088, CVE-2014-4089,
CVE-2014-4090, CVE-2014-4091, CVE-2014-4092, CVE-2014-4093, CVE-2014-4094,
CVE-2014-4095, CVE-2014-4096, CVE-2014-4097, CVE-2014-4098, CVE-2014-4099,

CVE-2014-4100, CVE-2014-4101, CVE-2014-4102, CVE-2014-4103, CVE-2014-4104,
CVE-2014-4105, CVE-2014-4106, CVE-2014-4107, CVE-2014-4108, CVE-2014-4109,
CVE-2014-4110, CVE-2014-4111, CVE-2014-4072, CVE-2014-4074, CVE-2014-4068,
CVE-2014-4070, CVE-2014-4071

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