CAIS-Alerta: Resumo dos Boletins de Segurança da Microsoft - Fevereiro/2015

[RNP, 12.02.2015]

A Microsoft publicou 9 boletins de segurança em 10 de fevereiro de 2015 que abordam ao todo 55 vulnerabilidades em produtos da empresa. As explorações destas vulnerabilidades permitem execução de código remota, desvio de recurso de segurança, divulgação de informações, elevação de privilégio e divulgação não autorizada de informação.

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

Severidade

Crítica

- MS15-009 - Atualização de segurança para o Internet Explorer
- MS15-010 - Vulnerabilidades no driver de modo kernel do Windows pode permitir a execução de código remoto
- MS15-011 - Vulnerabilidade na política de grupo pode permitir a execução de código remoto

Importante

- MS15-012 - Vulnerabilidades no Microsoft Office pode permitir a execução de código remoto
- MS15-013 - Vulnerabilidade no Microsoft Office pode permitir ignorar o recurso de segurança
- MS15-014 - Vulnerabilidade na política de grupo pode permitir ignorar o recurso de segurança
- MS15-015 - Vulnerabilidade no Microsoft Windows pode permitir a elevação de privilégio
- MS15-016 - Vulnerabilidade no Microsoft Graphics Component pode permitir a divulgação de informações
- MS15-017 - Vulnerabilidade no Virtual Machine Manager pode permitir a elevação de privilégio

Moderada

Nenhum boletim

Baixa

Nenhum boletim

O sistema de classificação de severidade das vulnerabilidades adotado pelo CAIS é o da própria Microsoft. O CAIS recomenda que se apliquem 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 fevereiro de 2015

https://technet.microsoft.com/pt-BR/library/security/ms15-feb.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):

CVE-2014-8967	CVE-2015-0028	CVE-2015-0042	CVE-2015-0054	CVE-2015-0058
CVE-2015-0017	CVE-2015-0029	CVE-2015-0043	CVE-2015-0055	CVE-2015-0059
CVE-2015-0018	CVE-2015-0030	CVE-2015-0044	CVE-2015-0066	CVE-2015-0008
CVE-2015-0019	CVE-2015-0031	CVE-2015-0045	CVE-2015-0067	CVE-2015-0063
CVE-2015-0020	CVE-2015-0035	CVE-2015-0046	CVE-2015-0068	CVE-2015-0064
CVE-2015-0021	CVE-2015-0036	CVE-2015-0048	CVE-2015-0069	CVE-2015-0065
CVE-2015-0022	CVE-2015-0037	CVE-2015-0049	CVE-2015-0070	CVE-2014-6362
CVE-2015-0023	CVE-2015-0038	CVE-2015-0050	CVE-2015-0071	CVE-2015-0009
CVE-2015-0025	CVE-2015-0039	CVE-2015-0051	CVE-2015-0003	CVE-2015-0062
CVE-2015-0026	CVE-2015-0040	CVE-2015-0052	CVE-2015-0010	CVE-2015-0061
CVE-2015-0027	CVE-2015-0041	CVE-2015-0053	CVE-2015-0057	CVE-2015-0012

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 **Twitter:**

Siga @caisrnp