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

[RNP, 15.01.2015]

A Microsoft publicou 8 boletins de segurança em 13 de janeiro de 2015 que abordam ao todo 8 vulnerabilidades em produtos da empresa. As explorações destas vulnerabilidades permitem execução de código remota, elevação de privilégio, ignorar recurso de segurança e negação de serviço.

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

Severidade

Crítica

- MS15-002 - Vulnerabilidade do serviço do Windows Telnet pode permitir a execução de código remoto

Importante

- MS15-001 - Vulnerabilidade no cache de compatibilidade de aplicativo do Windows pode permitir a elevação de privilégio
- MS15-003 - Vulnerabilidade do serviço do Windows User Profile pode permitir a elevação de privilégio
- MS15-004 - Vulnerabilidade no Windows Components pode permitir a elevação de privilégio
- MS15-005 - Vulnerabilidade no Network Location Awareness Service pode permitir ignorar recursos
- MS15-006 - Vulnerabilidade no Windows Error Reporting pode ignorar o recurso de segurança
- MS15-007 - Vulnerabilidade na implementação do Network Policy Server RADIUS Implementation pode causar negação de serviço
- MS15-008 - Vulnerabilidade no driver do modo Windows Kernel 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 janeiro de 2015

https://technet.microsoft.com/pt-BR/library/security/ms15-jan.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-2015-0002	CVE-2015-0004	CVE-2015-0006	CVE-2015-0015
CVE-2015-0014	CVE-2015-0016	CVE-2015-0001	CVE-2015-0011

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