CAIS-Alerta: Resumo dos Boletins de Segurança Microsoft - Fevereiro/2012

Microsoft Security Bulletin Summary for February 2012

[RNP, 17.02.2012-, revisão 01]

A Microsoft publicou 9 boletins de segurança em 15 de fevereiro que abordam ao todo 20 vulnerabilidades em produtos da empresa. A exploração destas vulnerabilidades permitem execução remota de código e elevação de privilégio.

Severidade

- **Crítica**
    - **MS12-008 - Vulnerabilidades em drivers do modo do kernel do Windows podem permitir execução remota de código.**
    - **MS12-010 - Atualização de segurança cumulativa para o Internet Explorer.**
    - **MS12-013 - Vulnerabilidade na Biblioteca de tempo de execução C pode permitir a execução remota de código.**
    - **MS12-016 - Vulnerabilidades no .NET Framework e no Microsoft Silverlight podem permitir execução remota de código.**
- **Importante**
    - **MS12-009 - Vulnerabilidades no Ancillary Function Driver podem permitir elevação de privilégio.**
    - **MS12-011 - Vulnerabilidades no Microsoft SharePoint podem permitir a elevação de privilégio.**
    - **MS12-012 - Vulnerabilidade no Painel de controle colorido pode permitir a execução remota de código.**
    - **MS12-014 - Vulnerabilidade no Codec da Indeo pode permitir a execução remota de código.**
    - **MS12-015 - Vulnerabilidades no Microsoft Visio Viewer 2010 podem permitir a execução remota de código.**
- **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 pode 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
- Windows Server Update Services

Mais informações

- Resumo do Boletim de Segurança da Microsoft de fevereiro 2012
- Microsoft TechCenter de Segurança
- Microsoft Security Response Center - MSRC
- Microsoft Security Research & Defense - MSRD
- Segurança Microsoft
- MS12-008 - Vulnerabilidades em drivers do modo do kernel do Windows podem permitir execução remota de código
- MS12-010 - Atualização de segurança cumulativa para o Internet Explorer
- MS12-013 - Vulnerabilidade na Biblioteca de tempo de execução C pode permitir a execução remota de código
- MS12-016 - Vulnerabilidades no .NET Framework e no Microsoft Silverlight podem permitir execução remota de código
- MS12-009 - Vulnerabilidades no Ancillary Function Driver podem permitir elevação de privilégio
- MS12-006 - Vulnerabilidade no SSL/TLS pode permitir divulgação não autorizada de informações
- MS12-011 - Vulnerabilidades no Microsoft SharePoint podem permitir a elevação de privilégio

- MS12-012 - Vulnerabilidade no Painel de controle colorido pode permitir a execução remota de código
- MS12-014 - Vulnerabilidade no Codec da Indeo pode permitir a execução remota de código
- MS12-015 - Vulnerabilidades no Microsoft Visio Viewer 2010 podem permitir a execução remota de código
- MS12-011 - Vulnerabilidades no Microsoft SharePoint podem permitir a elevação de privilégio

Identificador CVE (http://cve.mitre.org):
CVE-2011-0154, CVE-2012-5046, CVE-2012-0148, CVE-2012-0149, CVE-2012-0011, CVE-2012-0012, CVE-2012-0155, CVE-2012-0017, CVE-2012-0144, CVE-2012-0145, CVE-2012-5082, CVE-2012-0150, CVE-2012-0138, CVE-2012-0019, CVE-2012-0020, CVE-2012-0136, CVE-2012-0137, CVE-2012-0138, CVE-2012-0014, CVE-2012-0015,

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.