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

Microsoft Security Bulletin Summary for August 2012

[RNP, 15.08.2012-, revisão 01]

A Microsoft publicou 9 boletins de segurança em 14 de Agosto que abordam ao todo 15 vulnerabilidades em produtos da empresa. A exploração destas vulnerabilidades permitem execução remota de código e elevação de privilégio.

Até o momento da publicação deste alerta não há indícios de exploração ativa de nenhuma das vulnerabilidades citadas abaixo.

Severidade

- **Crítica**
    - **MS12-052 - Atualização cumulativa de segurança para Microsoft Internet Explorer**
    - **MS12-053 - Vulnerabilidade no recurso Remote Desktop pode permitir a execução remota de código**
    - **MS12-054 - Vulnerabilidade no Componente de Rede Windows pode permitir a execução remota de código**
    - **MS12-060 - Vulnerabilidade nos Controles Comuns do Windows pode permitir a execução remota de código**
    - **MS12-058 - Vulnerabilidade no recurso de visualização de documentos WebReady do Microsoft Exchange Server pode permitir a execução remota de código**
- **Importante**
    - **MS12-055 - Vulnerabilidades nos drivers kernel-mode do Windows podem permitir a elevação de privilégio**
    - **MS12-056 - Vulnerabilidades no funcionamento do JScript e VBScript podem permitir a execução remota de código**
    - **MS12-057 - Vulnerabilidade no Microsoft Office pode permitir a execução remota de código**
    - **MS12-059 - Vulnerabilidade no Microsoft Visio pode permitir a execução remota de código**
- **Moderada**
- **Nenhum boletim**
- **Baixa**

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 agosto 2012
- Microsoft TechCenter de Segurança
- Microsoft Security Response Center - MSRC
- Microsoft Security Research & Defense - MSRD
- Segurança Microsoft
- MS12-043 - Vulnerabilidade no Microsoft XML Core Services pode permitir execução remota de código

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

CVE-2012-1526 CVE-2012-2521 CVE-2012-2522 CVE-2012-2523 CVE-2012-2526

CVE-2012-1850 CVE-2012-1851 CVE-2012-1852 CVE-2012-1853 CVE-2012-2527

,

CVE-2012-2524 CVE-2012-1888 CVE-2012-1856CVE-2012-1894

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.

CENTRO DE ATENDIMENTO A INCIDENTES DE SEGURANCA (CAIS)

Rede Nacional de Ensino e Pesquisa (RNP)

cais@cais.rnp.br

http://www.cais.rnp.br

Tel. 019-3787-3300 Fax. 019-3787-3301

Chave PGP disponivel: http://www.rnp.br/cais/cais-pgp.key