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

Microsoft Security Bulletin Summary for June 2012

[RNP, 15.06.2012-, revisão 01]

A Microsoft publicou 7 boletins de segurança em 12 de junho que abordam ao todo 25 vulnerabilidades em produtos da empresa. A exploração destas vulnerabilidades permitem execução remota de código e elevação de privilégio.

AAté o momento da publicação deste alerta há exploração ativa de uma das vulnerabilidades, MS12-037.

Severidade

- **Crítica**
    - **MS12-036 - Vulnerabilidade no Microsoft Remote Desktop pode permitir a execução remota de código**
    - **MS12-037 - Atualização cumulativa de segurança para Microsoft Internet Explorert.**
    - **MS12-038 - Vulnerabilidade no .NET Framework pode permitir execução remota de código.**
- **Importante**
    - **MS12-039 - Vulnerabilidades no Lync Cloud podem permitir a execução remota de código.**
    - **MS12-040 - Vulnerabilidade no Microsoft Dynamics AX Enterprise Portal Could pode permitir a elevação de privilégio.**
    - **MS12-041 - Vulnerabilidades nos drivers kernel-mode do Windows podem permitir a elevação de privilégio.**
    - **MS12-042 - Vulnerabilidades no Windows Kernel Could podem permitir a elevação de privilégio.**
- **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 junho 2012
- Microsoft TechCenter de Segurança
- Microsoft Security Response Center - MSRC
- Microsoft Security Research & Defense - MSRD
- Segurança Microsoft
- MS12-036 - Vulnerabilidade no Microsoft Remote Desktop pode permitir a execução remota de código
- MS12-037 - Atualização cumulativa de segurança para Microsoft Internet Explorer
- MS12-038 - Vulnerabilidade no .NET Framework pode permitir execução remota de código
- MS12-039 - Vulnerabilidades no Lync Cloud podem permitir a execução remota de código
- MS12-040 - Vulnerabilidade no Microsoft Dynamics AX Enterprise Portal Could pode permitir a elevação de privilégio
- MS12-041 - Vulnerabilidades nos drivers kernel-mode do Windows podem permitir a elevação de privilégio
- MS12-042 - Vulnerabilidades no Windows Kernel Could podem permitir a elevação de privilégio

Identificador CVE (http://cve.mitre.org):
CVE-2012-0159, CVE-2012-0173, CVE-2012-0217, CVE-2012-1515,

CVE-2012-1523, CVE-2012-1849, CVE-2012-1855, CVE-2012-1857,CVE-2012-1858, CVE-2012-1858, CVE-2012-1864, CVE-2012-1865,CVE-2012-1866, CVE-2012-1867, CVE-2012-1868, CVE-2012-1873,CVE-2012-1874, CVE-2012-1875, CVE-2012-1876, CVE-2012-1877,CVE-2012-1878, CVE-2012-1879, CVE-2012-1880, CVE-2012-1881,CVE-2012-34021

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.