

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

Microsoft Security Bulletin Summary for April 2012

[RNP, 16.04.2012-, revisão 01]

A Microsoft publicou 6 boletins de segurança em 10 de abril que abordam ao todo 9 vulnerabilidades em produtos da empresa. A exploração destas vulnerabilidades permitem execução remota de código e divulgação não autorizada de informação.

Severidade

- **Crítica**
 - **MS12-023 - Atualização de segurança cumulativa para o Internet Explorer.**
 - **MS12-024 - Vulnerabilidade no Windows pode permitir a execução remota de código.**
 - **MS12-025 - Vulnerabilidade no .NET Framework pode permitir execução remota de código.**
 - **MS12-027 - Vulnerabilidades nos controles comuns do Windows podem permitir a execução remota de código.**
- **Importante**
 - **MS12-026 - Vulnerabilidades no Forefront Unified Access Gateway (UAG) podem permitir divulgação não autorizada de informações.**
 - **MS12-028 - Vulnerabilidade no Microsoft Office pode permitir a execução remota de código.**
 - **MS12-022 - Vulnerabilidades no Expression Design podem permitir execução remota de código.**
 - **MS12-019 - Vulnerabilidades no DirectWrite podem permitir negação de serviço.**
- **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 abril 2012](#)
- [Microsoft TechCenter de Segurança](#)
- [Microsoft Security Response Center - MSRC](#)
- [Microsoft Security Research & Defense - MSRD](#)
- [Segurança Microsoft](#)
- [MS12-023 - Atualização de segurança cumulativa para o Internet Explorer](#)
- [MS12-024 - Vulnerabilidade no Windows pode permitir a execução remota de código](#)
- [MS12-025 - Vulnerabilidade no .NET Framework pode permitir execução remota de código](#)
- [MS12-027 - Vulnerabilidades nos controles comuns do Windows podem permitir a execução remota de código](#)
- [MS12-026 - Vulnerabilidades no Forefront Unified Access Gateway \(UAG\) podem permitir divulgação não autorizada de informações](#)
- [MS12-028 - Vulnerabilidade no Microsoft Office pode permitir a execução remota de código](#)

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

CVE-2012-0169, CVE-2012-0170, CVE-2012-0172,

CVE-2012-0171, CVE-2012-0151, CVE-2012-0163, CVE-2012-0147, CVE-2012-0158,
CVE-2012-0177,

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](https://twitter.com/caisrnp).