CAIS-Alerta: Resumo dos Boletins de Segurança Microsoft - Julho/2014

Microsoft Security Bulletin Summary for July 2014

[RNP, 11.07.2014-, revisão 01]

A Microsoft publicou seis (6) boletins de segurança em 8 de julho de 2014 que abordam ao todo 27 vulnerabilidades em produtos da empresa. A exploração dessas vulnerabilidades permite a execução remota de código, a divulgação não autorizada de informação, a negação de serviço e a falsificação.

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

Severidade

- **Crítica**
    - **MS14-037 - Atualização de segurança cumulativa para o Internet Explorer**
    - **MS14-038 - Vulnerabilidade no Windows Journal pode permitir a execução remota de código**
- **Importante**
    - **MS14-039 - Vulnerabilidade no Teclado virtual pode permitir a elevação de privilégio**
    - **MS14-040 - Vulnerabilidade no Ancillary Function Driver (AFD) pode permitir elevação de privilégio**
    - **MS14-041 - Vulnerabilidade no DirectShow pode permitir elevação de privilégio**
- **Moderada**
- **MS14-042 - Vulnerabilidade no Microsoft Service Bus pode permitir negação de serviço**
- **Baixa**
- **Nenhum boletim**

O sistema de classificação de severidade das vulnerabilidades adotado pelo CAIS nesse 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 julho de 2014
- Microsoft TechCenter de Segurança
- Microsoft Security Response Center - MSRC
- Microsoft Security Research & Defense - MSRD
- Central de Proteção e Segurança Microsoft

Identificador CVE (http://cve.mitre.org):
CVE-2014-1763, CVE-2014-1765, CVE-2014-2785, CVE-2014-2786, CVE-2014-2787,
CVE-2014-2788, CVE-2014-2789, CVE-2014-2790, CVE-2014-2791, CVE-2014-2792,
CVE-2014-2794, CVE-2014-2795, CVE-2014-2797, CVE-2014-2798, CVE-2014-2800,
CVE-2014-2801, CVE-2014-2802, CVE-2014-2803, CVE-2014-2804, CVE-2014-2806,
CVE-2014-2807, CVE-2014-2809, CVE-2014-2813, CVE-2014-1824, CVE-2014-2781,
CVE-2014-1767, CVE-2014-2780

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.