CAIS-Alerta: Resumo dos Boletins de Segurança Microsoft - Agosto/2013

Microsoft Security Bulletin Summary for August 2013

[RNP, 20.08.2013-, revisão 01]

A Microsoft publicou 8 boletins de segurança em 13 de agosto de 2013 que abordam ao todo 19 vulnerabilidades em produtos da empresa. A exploração dessas vulnerabilidades permite execução remota de código e elevação de privilégio. Até o momento da publicação deste alerta, não foram divulgados códigos de exploração para as vulnerabilidades listadas.

Severidade

- **Crítica**
- **- MS13-059 - Atualização de segurança cumulativa para o Internet Explorer**
- **- MS13-060 - Vulnerabilidade no Processador de Scripts Unicode pode permitir a execução remota de código**
- **- MS13-061 - Vulnerabilidades no Microsoft Exchange Server podem permitir a execução remota de código**

- **Importante**
- **- MS13-062 - Vulnerabilidade em chamada de procedimento remoto pode permitir elevação de privilégio**
- **- MS13-063 - Vulnerabilidades no kernel do Windows podem permitir a elevação de privilégio**
- **- MS13-064 - Vulnerabilidade em Windows NAT Driver poderá permitir negação de serviço**
- **- MS13-065 - Vulnerabilidade no ICMPv6 pode permitir negação de serviço**
- **- MS13-066 - Vulnerabilidade nos Servi?os de Federação do Active Directory pode permitir divulgação não autorizada de informação**

- **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 possa 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
- Microsoft Download Center

Mais informações

- Resumo do Boletim de Segurança da Microsoft de agosto de 2013 (em inglês)
- 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-2013-3184, CVE-2013-3187, CVE-2013-3188, CVE-2013-3189, CVE-2013-3190, CVE-2013-3191, CVE-2013-3193, CVE-2013-3194, CVE-2013-3199, CVE-2013-3181, CVE-2013-3175, CVE-2013-2556, CVE-2013-3196, CVE-2013-3197, CVE-2013-3198, CVE-2013-3182, CVE-2013-3183, CVE-2013-3185

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