**CAIS-Alerta: Resumo dos Boletins de Segurança da Microsoft - Abril/2015**

[RNP, 22.04.2015]

A Microsoft publicou 11 boletins de segurança em 14 de abril de 2015 que abordam ao todo 26 vulnerabilidades em produtos da empresa. As explorações destas vulnerabilidades permitem **execução de código remota**, **desvio de recurso de segurança**, **divulgação de informações**, **elevação de privilégio**, **divulgação não autorizada de informação**, **desvio de recurso de segurança** e **negação de serviço**.

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

**Severidade**

**Crítica**

- MS15-032 - Atualização de Segurança Cumulativa para o Internet Explorer
- MS15-033 - Vulnerabilidades no Microsoft Office podem permitir a Execução de código remota
- MS15-034 - Vulnerabilidade no HTTP.sys pode permitir a Execução de código remota
- MS15-035 - Vulnerabilidade no componente do Microsoft Graphics pode permitir a Execução de código remota

**Importante**

- MS15-036 - Vulnerabilidades no Microsoft SharePoint Server podem permitir a elevação de privilégio
- MS15-037 - Vulnerabilidade no Agendador de Tarefas do Windows pode permitir a elevação de privilégio
- MS15-038 - Vulnerabilidades no Microsoft Windows podem permitir a elevação de privilégio
- MS15-039 - Vulnerabilidade no XML Core Services pode permitir que o recurso de segurança seja ignorado
- MS15-040 - Vulnerabilidade nos Serviços de Federação do Active Directory pode permitir a divulgação de informações
- MS15-041 - Vulnerabilidade no .Net Framework pode permitir a divulgação não autorizada de informações
- MS15-042 - Vulnerabilidade no Windows Hyper-V pode permitir a negação de serviço

**Moderada**

Nenhum boletim

**Baixa**

Nenhum boletim

O sistema de classificação de severidade das vulnerabilidades adotado pelo CAIS é o da própria Microsoft. O CAIS recomenda que se apliquem 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

https://www.update.microsoft.com/microsoftupdate

Microsoft Download Center

http://www.microsoft.com/en-us/download/default.aspx

**Mais informações**

Resumo do Boletim de Segurança da Microsoft de abril de 2015

https://technet.microsoft.com/pt-BR/library/security/ms15-apr.aspx

Microsoft TechCenter de Segurança

https://technet.microsoft.com/pt-br/security

Microsoft Security Response Center - MSRC

https://technet.microsoft.com/pt-br/security/dn440717

Microsoft Security Research & Defense - MSRD

http://blogs.technet.com/b/srd/

Central de Proteção e Segurança Microsoft

https://www.microsoft.com/pt-br/security/default.aspx

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

| | | | | |
|---|---|---|---|---|
| CVE-2015-1652 | CVE-2015-1665 | CVE-2015-1641 | CVE-2015-1645 | CVE-2015-1644 |
| CVE-2015-1657 | CVE-2015-1666 | CVE-2015-1649 | CVE-2015-1640 | CVE-2015-1646 |
| CVE-2015-1659 | CVE-2015-1667 | CVE-2015-1650 | CVE-2015-1653 | CVE-2015-1638 |
| CVE-2015-1660 | CVE-2015-1668 | CVE-2015-1651 | CVE-2015-0098 | CVE-2015-1648 |
| CVE-2015-1661 | CVE-2015-1639 | CVE-2015-1635 | CVE-2015-1643 | CVE-2015-1647 |
| CVE-2015-1662 | | | | |

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 **Twitter:**

**Siga @caisrnp**