

## CAIS-Alerta: Resumo dos Boletins de Segurança da Microsoft - Junho/2015

[RNP, 10.06.2015]

A Microsoft publicou 8 boletins de segurança em 9 de junho de 2015 que abordam ao todo 45 vulnerabilidades em produtos da empresa. As explorações destas vulnerabilidades permitem **execução de código remota e elevação de privilégio**.

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

### Severidade

#### Crítica

- MS15-056 - Atualização de Segurança Cumulativa para o Internet Explorer
- MS15-057 - Vulnerabilidade no Windows Media Player pode permitir a execução remota de código

#### Importante

- MS15-059 - Vulnerabilidades no Microsoft Office podem permitir a Execução de código remota
- MS15-060 - Vulnerabilidade nos controles comuns da Microsoft pode permitir a execução remota de código
- MS15-061 - Vulnerabilidades em drivers do modo do kernel do Windows podem permitir a elevação de privilégio
- MS15-062 - Vulnerabilidade nos Serviços de Federação do Active Directory pode permitir a elevação de privilégio
- MS15-063 - Vulnerabilidade no Kernel do Windows pode permitir a elevação de privilégio
- MS15-064 - Vulnerabilidades no servidor do Microsoft Exchange podem permitir a elevação de privilégio

#### 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 junho de 2015

<https://technet.microsoft.com/pt-br/library/security/ms15-jun.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-2015-1687	CVE-2015-1741	CVE-2015-1752	CVE-2015-1770	CVE-2015-1726
CVE-2015-1730	CVE-2015-1742	CVE-2015-1753	CVE-2015-1756	CVE-2015-1727
CVE-2015-1731	CVE-2015-1743	CVE-2015-1754	CVE-2015-1719	CVE-2015-1768
CVE-2015-1732	CVE-2015-1744	CVE-2015-1755	CVE-2015-1720	CVE-2015-2360
CVE-2015-1735	CVE-2015-1745	CVE-2015-1765	CVE-2015-1721	CVE-2015-1757
CVE-2015-1736	CVE-2015-1747	CVE-2015-1766	CVE-2015-1722	CVE-2015-1758
CVE-2015-1737	CVE-2015-1748	CVE-2015-1728	CVE-2015-1723	CVE-2015-1764
CVE-2015-1739	CVE-2015-1750	CVE-2015-1759	CVE-2015-1724	CVE-2015-1771
CVE-2015-1740	CVE-2015-1751	CVE-2015-1760	CVE-2015-1725	CVE-2015-2359

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**