

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

[RNP, 15.07.2015]

A Microsoft publicou 14 boletins de segurança em 14 de julho de 2015 que abordam ao todo 59 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

- MS15-065 – Atualização de segurança para Internet Explorer
- MS15-066 – Vulnerabilidade no VBScript Scripting Engine pode permitir execução remota de código
- MS15-067 – Vulnerabilidade no RDP pode permitir execução remota de código
- MS15-068 – Vulnerabilidades no Windows Hyper-V pode permitir execução remota de código

#### Importante

- MS15-058 – Vulnerabilidades no SQL Server pode permitir execução remota de código
- MS15-069 – Vulnerabilidades no Windows podem permitir execução remota de código
- MS15-070 – Vulnerabilidades no Microsoft Office podem permitir execução remota de código
- MS15-071 – Vulnerabilidade no Netlogon pode permitir elevação de privilégio
- MS15-072 – Vulnerabilidade no Windows Graphics Component pode permitir elevação de privilégio
- MS15-073 – Vulnerabilidade no Windows Kernel-Mode Driver pode permitir elevação de privilégio
- MS15-074 – Vulnerabilidade no Windows Installer Service pode permitir elevação de privilégio
- MS15-075 – Vulnerabilidades no OLE podem permitir elevação de privilégio
- MS15-076 – Vulnerabilidade no Windows Remote Procedure Call pode permitir elevação de privilégio
- MS15-077 – Vulnerabilidade no ATM Font Driver pode permitir 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 julho de 2015

<https://technet.microsoft.com/pt-BR/library/security/ms15-jul.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-2015-1761	CVE-2015-2389	CVE-2015-2411	CVE-2015-2368	CVE-2015-2363
CVE-2015-1762	CVE-2015-2390	CVE-2015-2412	CVE-2015-2369	CVE-2015-2365
CVE-2015-1763	CVE-2015-2391	CVE-2015-2413	CVE-2015-2375	CVE-2015-2366
CVE-2015-1729	CVE-2015-2397	CVE-2015-2414	CVE-2015-2376	CVE-2015-2367
CVE-2015-1733	CVE-2015-2398	CVE-2015-2419	CVE-2015-2377	CVE-2015-2381
CVE-2015-1738	CVE-2015-2401	CVE-2015-2421	CVE-2015-2378	CVE-2015-2382
CVE-2015-1767	CVE-2015-2402	CVE-2015-2422	CVE-2015-2379	CVE-2015-2371
CVE-2015-2372	CVE-2015-2403	CVE-2015-2425	CVE-2015-2380	CVE-2015-2416
CVE-2015-2383	CVE-2015-2404	CVE-2015-2372	CVE-2015-2415	CVE-2015-2417
CVE-2015-2384	CVE-2015-2406	CVE-2015-2373	CVE-2015-2424	CVE-2015-2370
CVE-2015-2385	CVE-2015-2408	CVE-2015-2361	CVE-2015-2374	CVE-2015-2387
CVE-2015-2388	CVE-2015-2410	CVE-2015-2362	CVE-2015-2364	

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**