

## CAIS-Alerta: Resumo dos Boletins de Segurança da Microsoft - Agosto/2016

[RNP, 09.08.2016]

A Microsoft publicou 9 boletins de segurança em 9 de agosto de 2016 que abordam ao todo 34 vulnerabilidades em produtos da empresa. As explorações destas vulnerabilidades permitem **execução remota de código, elevação de privilégio, divulgação não autorizada de informações e *bypass* do recurso de segurança**. Até o momento da publicação deste alerta não foram divulgados códigos de exploração para as vulnerabilidades listadas.

### Severidade

#### Crítica

- MS16-095 - Atualização de segurança cumulativa para o Internet Explorer
- MS16-096 - Atualização de segurança cumulativa do Microsoft Edge
- MS16-097 - Atualização de segurança para o componente gráfico da Microsoft
- MS16-099 - Atualização de segurança para o Microsoft Office
- MS16-102 - Atualização de segurança para a biblioteca de PDFs do Microsoft Windows

#### Importante

- MS16-098 - Atualização de segurança para drivers do modo Kernel do Windows
- MS16-100 - Atualização de segurança para a Inicialização Segura
- MS16-101 - Atualização de segurança para métodos de autenticação do Windows
- MS16-103 - Atualização de segurança para ActiveSyncProvider

#### 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 agosto de 2016

<https://technet.microsoft.com/pt-br/library/security/ms16-aug.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-2016-3288	CVE-2016-3327	CVE-2016-3326	CVE-2016-3309	CVE-2016-3318
CVE-2016-3289	CVE-2016-3329	CVE-2016-3327	CVE-2016-3310	CVE-2016-3320
CVE-2016-3290	CVE-2016-3289	CVE-2016-3329	CVE-2016-3311	CVE-2016-3237
CVE-2016-3293	CVE-2016-3293	CVE-2016-3301	CVE-2016-3313	CVE-2016-3300
CVE-2016-3321	CVE-2016-3296	CVE-2016-3303	CVE-2016-3315	CVE-2016-3319
CVE-2016-3322	CVE-2016-3319	CVE-2016-3304	CVE-2016-3316	CVE-2016-3312
CVE-2016-3326	CVE-2016-3322	CVE-2016-3308	CVE-2016-3317	

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**