

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

[RNP, 09.12.2015]

A Microsoft publicou 12 boletins de segurança em 8 de dezembro de 2015 que abordam ao todo 71 vulnerabilidades em produtos da empresa. As explorações destas vulnerabilidades permitem **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

- MS15-124 - Atualização de Segurança Cumulativa para o Internet Explorer
- MS15-125 - Atualização de segurança cumulativa do Microsoft Edge
- MS15-126 - Atualização de segurança cumulativa para JScript e VBScript para corrigir a execução remota de código
- MS15-127 - Atualização de segurança de DNS do Microsoft Windows para corrigir execução remota de código
- MS15-128 - Atualização de segurança de componente gráfico da Microsoft para corrigir execução remota de código
- MS15-129 - Atualização de segurança do Silverlight para corrigir execução remota de código
- MS15-130 - Atualização de segurança do Microsoft Uniscribe para corrigir execução remota de código
- MS15-131 - Atualização de segurança do Microsoft Office para corrigir execução remota de código

Importante

- MS15-132 - Atualização de segurança do Microsoft Windows para corrigir execução remota de código
- MS15-133 - Atualização de segurança de PGM no Windows para corrigir elevação de privilégio
- MS15-134 - Atualização de segurança do Windows Media Center para corrigir execução remota de código
- MS15-135 - Atualização de segurança dos drivers de modo kernel do Windows para corrigir 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 dezembro de 2015

<https://technet.microsoft.com/pt-br/library/security/ms15-dec.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-2015-6083	CVE-2015-6149	CVE-2015-6164	CVE-2015-6170	CVE-2015-6122
CVE-2015-6134	CVE-2015-6150	CVE-2015-6139	CVE-2015-6176	CVE-2015-6124
CVE-2015-6135	CVE-2015-6151	CVE-2015-6140	CVE-2015-6135	CVE-2015-6172
CVE-2015-6136	CVE-2015-6152	CVE-2015-6142	CVE-2015-6136	CVE-2015-6177
CVE-2015-6138	CVE-2015-6153	CVE-2015-6148	CVE-2015-6125	CVE-2015-6128
CVE-2015-6139	CVE-2015-6154	CVE-2015-6151	CVE-2015-6106	CVE-2015-6132
CVE-2015-6140	CVE-2015-6155	CVE-2015-6153	CVE-2015-6107	CVE-2015-6133
CVE-2015-6141	CVE-2015-6156	CVE-2015-6154	CVE-2015-6108	CVE-2015-6126
CVE-2015-6142	CVE-2015-6157	CVE-2015-6155	CVE-2015-6114	CVE-2015-6127
CVE-2015-6143	CVE-2015-6158	CVE-2015-6158	CVE-2015-6165	CVE-2015-6131
CVE-2015-6144	CVE-2015-6159	CVE-2015-6159	CVE-2015-6166	CVE-2015-6171
CVE-2015-6145	CVE-2015-6160	CVE-2015-6161	CVE-2015-6130	CVE-2015-6173
CVE-2015-6146	CVE-2015-6161	CVE-2015-6168	CVE-2015-6040	CVE-2015-6174
CVE-2015-6147	CVE-2015-6162	CVE-2015-6169	CVE-2015-6118	CVE-2015-6175
CVE-2015-6148				

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