

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

[RNP, 12.11.2015]

A Microsoft publicou 12 boletins de segurança em 10 de novembro de 2015 que abordam ao todo 33 vulnerabilidades em produtos da empresa. As explorações destas vulnerabilidades permitem **execução remota de código, elevação de privilégio, divulgação de informações, negação de serviço, falsificação, desvio de recurso de segurança**.

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

Severidade

Crítica

- MS15-112 - Atualização de Segurança Cumulativa para o Internet Explorer
- MS15-113 - Atualização de segurança cumulativa do Microsoft Edge
- MS15-114 - Atualização de segurança para o Windows Journal para abordar a execução remota de código
- MS15-115 - Atualização de segurança para o Microsoft Windows para abordar a execução remota de código

Importante

- MS15-116 - Atualização de segurança para Microsoft Office para abordar a execução remota de código
- MS15-117 - Atualização de segurança do NDIS para abordar a elevação de privilégio
- MS15-118 - Atualização de segurança do .NET Framework para abordar a elevação de privilégio
- MS15-119 - Atualização de segurança do Winsock para abordar a elevação de privilégio
- MS15-120 - Atualização de segurança do IPSec para abordar negação de serviço
- MS15-121 - Atualização de segurança do Schannel para abordar falsificação
- MS15-122 - Atualização de segurança do Kerberos para abordar desvio de recurso de segurança
- MS15-123 - Atualização de segurança do Skype for Business e Microsoft Lync para abordar divulgação de informações

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 novembro de 2015

<https://technet.microsoft.com/pt-BR/library/security/ms15-nov.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-2015-2427	CVE-2015-6075	CVE-2015-6087	CVE-2015-6103	CVE-2015-6123
CVE-2015-6064	CVE-2015-6076	CVE-2015-6088	CVE-2015-6104	CVE-2015-6098
CVE-2015-6065	CVE-2015-6077	CVE-2015-6089	CVE-2015-6109	CVE-2015-6096
CVE-2015-6066	CVE-2015-6078	CVE-2015-6064	CVE-2015-6113	CVE-2015-6099
CVE-2015-6068	CVE-2015-6079	CVE-2015-6073	CVE-2015-2503	CVE-2015-6115
CVE-2015-6069	CVE-2015-6080	CVE-2015-6078	CVE-2015-6038	CVE-2015-2478
CVE-2015-6070	CVE-2015-6081	CVE-2015-6088	CVE-2015-6091	CVE-2015-6111
CVE-2015-6071	CVE-2015-6082	CVE-2015-6097	CVE-2015-6092	CVE-2015-6112
CVE-2015-6072	CVE-2015-6084	CVE-2015-6100	CVE-2015-6093	CVE-2015-6095
CVE-2015-6073	CVE-2015-6085	CVE-2015-6101	CVE-2015-6094	CVE-2015-6061
CVE-2015-6074	CVE-2015-6086	CVE-2015-6102		

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