

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

[RNP, 14.05.2015]

A Microsoft publicou 13 boletins de segurança em 12 de maio de 2015 que abordam ao todo 48 vulnerabilidades em produtos da empresa. As explorações destas vulnerabilidades permitem **execução de código remota, desvio de recurso de segurança, elevação de privilégio, divulgação não autorizada de informação e negação de serviço**.

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

Severidade

Crítica

- MS15-043 - Atualização de Segurança Cumulativa para o Internet Explorer
- MS15-044 - Vulnerabilidades nos Drivers de fonte da Microsoft podem permitir a execução remota de código
- MS15-045 - Vulnerabilidade no Diário do Windows pode permitir a execução remota de código

Importante

- MS15-046 - Vulnerabilidades no Microsoft Office pode permitir a execução remota de código
- MS15-047 - Vulnerabilidades no Microsoft SharePoint Server podem permitir a execução remota de código
- MS15-048 - Vulnerabilidades no .NET Framework podem permitir elevação de privilégio
- MS15-049 - Vulnerabilidade no Silverlight pode permitir a elevação de privilégio
- MS15-050 - Vulnerabilidade no Gerenciador de Controle de Serviços pode permitir a elevação de privilégio
- MS15-051 - Vulnerabilidades nos drivers do modo kernel do Windows podem permitir a elevação de privilégio
- MS15-052 - Vulnerabilidade no kernel do Windows pode permitir o desvio do recurso de segurança
- MS15-053 - Vulnerabilidades nos mecanismos de script do JScript e VBScript poderiam permitir o desvio de recurso de segurança
- MS15-054 - Vulnerabilidade no formato de arquivo do Console de Gerenciamento Microsoft pode permitir negação de serviço

- MS15-055 - Vulnerabilidade no Schannel pode permitir a divulgação não autorizada de informação

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 maio de 2015

<https://technet.microsoft.com/pt-BR/library/security/ms15-may.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-2015-1658	CVE-2015-1704	CVE-2015-1717	CVE-2015-1682	CVE-2015-1679
CVE-2015-1684	CVE-2015-1705	CVE-2015-1718	CVE-2015-1683	CVE-2015-1680
CVE-2015-1685	CVE-2015-1706	CVE-2015-1670	CVE-2015-1700	CVE-2015-1701
CVE-2015-1686	CVE-2015-1708	CVE-2015-1671	CVE-2015-1672	CVE-2015-1674
CVE-2015-1688	CVE-2015-1709	CVE-2015-1675	CVE-2015-1673	CVE-2015-1684
CVE-2015-1689	CVE-2015-1710	CVE-2015-1695	CVE-2015-1715	CVE-2015-1686
CVE-2015-1691	CVE-2015-1711	CVE-2015-1696	CVE-2015-1702	CVE-2015-1681
CVE-2015-1692	CVE-2015-1712	CVE-2015-1697	CVE-2015-1676	CVE-2015-1716
CVE-2015-1694	CVE-2015-1713	CVE-2015-1698	CVE-2015-1677	
CVE-2015-1703	CVE-2015-1714	CVE-2015-1699	CVE-2015-1678	

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