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

[RNP, 11.03.2015]

A Microsoft publicou 14 boletins de segurança em 10 de março de 2015 que abordam ao todo 45 vulnerabilidades em produtos da empresa. As explorações destas vulnerabilidades permitem execução de código remota, desvio de recurso de segurança, divulgação de informações, elevação de privilégio, divulgação não autorizada de informação, negação de serviço e falsificação.

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

Severidade

Crítica

- MS15-018 - Atualização de Segurança Cumulativa para o Internet Explorer
- MS15-019 - Vulnerabilidade no mecanismo de script VBScript pode permitir a execução de código remoto
- MS15-020 - Vulnerabilidade no Microsoft Windows pode permitir a execução remota de código
- MS15-021 - Vulnerabilidades no Driver de fonte da Adobe podem permitir a execução remota de código
- MS15-022 - Vulnerabilidades no Microsoft Office podem permitir a execução remota de código

Importante

- MS15-023 - Vulnerabilidades no driver de modo kernel podem permitir a elevação de privilégio
- MS15-024 - Vulnerabilidade no processamento de PNG pode permitir a divulgação de informações
- MS15-025 - Vulnerabilidades no kernel do Windows podem permitir elevação de privilégio
- MS15-026 - Vulnerabilidades no Microsoft Exchange Server podem permitir a elevação de privilégio
- MS15-027 - Vulnerabilidade no NETLOGON pode permitir falsificação
- MS15-028 - Vulnerabilidade no Agendador de Tarefas do Windows pode permitir o desvio do recurso de segurança
- MS15-029 - Vulnerabilidade no componente de decodificador de fotos do Windows pode permitir a divulgação de informações
- MS15-030 - Vulnerabilidade no Protocolo RDP Pode permitir Negação de Serviço

- MS15-031 - Vulnerabilidade no Schannel pode permitir o desvio do recurso de segurança

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 março de 2015

https://technet.microsoft.com/pt-br/library/security/ms15-mar.aspx

Microsoft TechCenter de Segurança

http://technet.microsoft.com/pt-br/security

Microsoft Security Response Center - MSRC

http://www.microsoft.com/security/msrc

Microsoft Security Research & Defense - MSRD

http://blogs.technet.com/srd

Central de Proteção e Segurança Microsoft

http://www.microsoft.com/brasil/security

Identificador CVE (http://cve.mitre.org):

CVE-2015-0032	CVE-2015-1625	CVE-2015-0087	CVE-2015-0086	CVE-2015-0080
CVE-2015-0056	CVE-2015-1626	CVE-2015-0088	CVE-2015-0097	CVE-2015-0073
CVE-2015-0072	CVE-2015-1627	CVE-2015-0089	CVE-2015-1633	CVE-2015-0075
CVE-2015-0099	CVE-2015-1634	CVE-2015-0090	CVE-2015-1636	CVE-2015-1628
CVE-2015-0100	CVE-2015-0032	CVE-2015-0091	CVE-2015-0077	CVE-2015-1629
CVE-2015-1622	CVE-2015-0081	CVE-2015-0092	CVE-2015-0078	CVE-2015-1630
CVE-2015-1623	CVE-2015-0096	CVE-2015-0093	CVE-2015-0094	CVE-2015-1631
CVE-2015-1624	CVE-2015-0074	CVE-2015-0085	CVE-2015-0095	CVE-2015-1632
CVE-2015-0005	CVE-2015-0084	CVE-2015-0076	CVE-2015-0079	CVE-2015-1637

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