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

[RNP, 10.09.2015]

A Microsoft publicou 12 boletins de segurança em 8 de setembro de 2015 que abordam ao todo 55 vulnerabilidades em produtos da empresa. As explorações destas vulnerabilidades permitem **execução remota de código, negação de serviço, elevação de privilégio, divulgação de informações** e **desvio de recurso de segurança**.

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

Severidade

Crítica

- MS15-094 - Atualização de segurança cumulativa para o Internet Explorer
- MS15-095 - Atualização de segurança cumulativa do Microsoft Edge
- MS15-097 - Vulnerabilidades no componente do Microsoft Graphics podem permitir a execução remota de código
- MS15-098 - Vulnerabilidade no Diário do Windows pode permitir a execução remota de código

Importante

- MS15-096 - Vulnerabilidade no Active Directory pode permitir uma negação de serviço
- MS15-099 - Vulnerabilidades no Microsoft Office pode permitir a execução remota de código
- MS15-100 - Vulnerabilidade no Windows Media Center pode permitir a execução remota de código
- MS15-101 - Vulnerabilidades no .NET Framework podem permitir elevação de privilégio
- MS15-102 - Vulnerabilidade no Agendador de Tarefas do Windows pode permitir a elevação de privilégio
- MS15-103 - Vulnerabilidade no Microsoft Exchange Server pode permitir a divulgação de Informações
- MS15-104 - Vulnerabilidades no Skype for Business Server e no Lync Server podem permitir a elevação de privilégio
- MS15-105 - Vulnerabilidade no Windows Hyper-V 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 setembro de 2015

https://technet.microsoft.com/pt-br/library/security/ms15-sep.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-2015-2483	CVE-2015-2498	CVE-2015-2506	CVE-2015-2513	CVE-2015-2526
CVE-2015-2484	CVE-2015-2499	CVE-2015-2507	CVE-2015-2514	CVE-2015-2524
CVE-2015-2485	CVE-2015-2500	CVE-2015-2508	CVE-2015-2516	CVE-2015-2525
CVE-2015-2486	CVE-2015-2501	CVE-2015-2510	CVE-2015-2519	CVE-2015-2528
CVE-2015-2487	CVE-2015-2541	CVE-2015-2511	CVE-2015-2530	CVE-2015-2505
CVE-2015-2489	CVE-2015-2542	CVE-2015-2512	CVE-2015-2520	CVE-2015-2543
CVE-2015-2490	CVE-2015-2485	CVE-2015-2517	CVE-2015-2521	CVE-2015-2544
CVE-2015-2491	CVE-2015-2486	CVE-2015-2518	CVE-2015-2522	CVE-2015-2531
CVE-2015-2492	CVE-2015-2494	CVE-2015-2527	CVE-2015-2523	CVE-2015-2532
CVE-2015-2493	CVE-2015-2542	CVE-2015-2529	CVE-2015-2509	CVE-2015-2536
CVE-2015-2494	CVE-2015-2535	CVE-2015-2546	CVE-2015-2504	CVE-2015-2534

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