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

[RNP, 12.08.2015]

A Microsoft publicou 13 boletins de segurança em 11 de agosto de 2015 que abordam ao todo 58 vulnerabilidades em produtos da empresa. As explorações destas vulnerabilidades permitem **execução de código remota**, **elevação de privilégio** e **divulgação de informações**.

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

Severidade

Crítica

- MS15-079 – Atualização de segurança para Internet Explorer
- MS15-080 – Vulnerabilidades no Microsoft Graphics Component pode permitir execução de código remota
- MS15-081 – Vulnerabilidades no Microsoft Office pode permitir execução de código remota
- MS15-091 – Atualização de segurança para Microsoft Edge

Importante

- MS15-082 – Vulnerabilidades no RDP pode permitir execução de código remota
- MS15-083 – Vulnerabilidade no Server Message Block pode permitir execução de código remota
- MS15-084 – Vulnerabilidades no XML Core Services pode permitir divulgação de informações
- MS15-085 – Vulnerabilidade no Mount Manager pode permitir elevação de privilégio
- MS15-086 – Vulnerabilidade no System Center Operations Manager pode permitir elevação de privilégio
- MS15-087 – Vulnerabilidade no UDDI Services pode permitir elevação de privilégio
- MS15-088 – Errôneo Command Line Parameter Passing pode permitir divulgação de informações
- MS15-089 – Vulnerabilidade no WebDAV pode permitir divulgação de informações
- MS15-090 – Vulnerabilidades no Microsoft Windows pode permitir 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 agosto de 2015

https://technet.microsoft.com/pt-BR/library/security/ms15-aug.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-2015-2423	CVE-2015-2452	CVE-2015-2461	CVE-2015-2477	CVE-2015-2476
CVE-2015-2441	CVE-2015-2431	CVE-2015-2462	CVE-2015-2472	CVE-2015-2428
CVE-2015-2442	CVE-2015-2432	CVE-2015-2463	CVE-2015-2473	CVE-2015-2429
CVE-2015-2443	CVE-2015-2433	CVE-2015-2464	CVE-2015-2474	CVE-2015-2430
CVE-2015-2444	CVE-2015-2435	CVE-2015-2465	CVE-2015-2434	CVE-2015-2441
CVE-2015-2445	CVE-2015-2453	CVE-2015-1642	CVE-2015-2440	CVE-2015-2442
CVE-2015-2446	CVE-2015-2454	CVE-2015-2423	CVE-2015-2471	CVE-2015-2446
CVE-2015-2447	CVE-2015-2455	CVE-2015-2466	CVE-2015-1769	CVE-2015-2449
CVE-2015-2448	CVE-2015-2456	CVE-2015-2467	CVE-2015-2420	CVE-2015-2479
CVE-2015-2449	CVE-2015-2458	CVE-2015-2468	CVE-2015-2475	CVE-2015-2480
CVE-2015-2450	CVE-2015-2459	CVE-2015-2469	CVE-2015-2423	CVE-2015-2481
CVE-2015-2451	CVE-2015-2460	CVE-2015-2470		

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