-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA256

CAIS-Alerta [18/04/2019]: Vulnerabilidade no Sistema Operacional Windows

Prezados,

O CAIS alerta para a recente vulnerabilidade crítica encontrada no kernel do sistema operacional Microsoft Windows, que pode permitir a escalada de privilégios. Já foram publicados códigos de exploração para a vulnerabilidade identificada.

DESCRIÇÃO

A vulnerabilidade pode permitir um usuário malicioso escalar privilégios no sistema operacional através da exploração de uma falha no componente Win32k.sys do sistema operacional. Este componente executa a função que define as classes gráficas - como barra de rolagem, menu, botões, etc. - das janelas criadas pelo sistema operacional Windows. O usuário pode executar um arquivo malicioso especialmente desenvolvido para explorar a falha na manipulação dos objetos em memória (use-after-free) do sistema pelo Win32k e, com isso aumentar privilégios no sistema operacional, assumir o controle do sistema afetado e executar comandos em modo kernel, tais como instalar programas, visualizar, alterar ou apagar dados, criar novas contas e alterar direitos de acessos de outros usuários. Para explorar a vulnerabilidade, o usuário malicioso precisa fazer previamente logon no sistema.

SISTEMAS IMPACTADOS

Sistemas Operacionais Microsoft Windows

VERSÕES AFETADAS

Microsoft Windows 7 Service Pack 1
Microsoft Windows 10
Microsoft Windows 10 v1607
Microsoft Windows 10 v1703
Microsoft Windows 10 v1709
Microsoft Windows 10 v1803
Microsoft Windows 10v1809
Microsoft Windows 8.1
Microsoft Windows RT 8.1
Microsoft Windows Server 2008
Microsoft Windows Server 2008 SP2 itanium
Microsoft Windows Server 2008 R2 Service Pack 1 itanium
Microsoft Windows Server 2008 R2 Service Pack 1 x64
Microsoft Windows Server 2012
Microsoft Windows Server 2012 R2

Microsoft Windows Server 2016
Microsoft Windows Server 2016 v1709
Microsoft Windows Server 2016 v1803
Microsoft Windows Server 2019

CORREÇÕES DISPONÍVEIS

Aplicar os patches de atualização fornecidos pela Microsoft [2].

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

CVE-2019-0859

MAIS INFORMAÇÕES

[1] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-0859
[2] https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0859
[3] https://www.kaspersky.com/blog/cve-2019-0859-detected/26451/
[4] https://securityaffairs.co/wordpress/83903/hacking/cve-2019-0803-windows-flaw.html
[5] https://nvd.nist.gov/vuln/detail/CVE-2019-0859

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 podem ser acompanhadas pelas redes sociais da RNP. Siga-nos!
Twitter: @RedeRNP
Facebook: facebook.com/RedeNacionaldeEnsinoePesquisaRNP.

Atenciosamente,

CAIS/RNP

###
CENTRO DE ATENDIMENTO A INCIDENTES DE SEGURANCA (CAIS)
Rede Nacional de Ensino e Pesquisa (RNP)
#   #
cais@cais.rnp.br   http://www.rnp.br/servicos/seguranca
Tel. 019-37873300   Fax. 019-37873301
Chave PGP disponivel   https://www.cais.rnp.br/cais-pgp.key
###

-----BEGIN PGP SIGNATURE-----
Version: OpenPGP.js v2.6.2
Comment: https://openpgpjs.org

wsFcBAEBCAAQBQJcuJqlCRB83qA0uPj0mAAAU5kP/iNPn4qiGYZ9flrzy+Sn
d6QWNT2bjFVjqd5HH3OS9T2B9cwrokADJi9P7LGb9HPjWbw0NeBfSPxvnjBQ

```
7OBPD2qX/2GV1TSWQsz4AqUXaGICo5+inRUB1OgkjTltW+0kjYnG0pDhq/Ii
aXjifBuqrJwiFgKjCH1bZ/IiN1XrsvVsgUzooGqjX/HPu2/nemy7V/JVg5X3
blkQsPJ0uVbq/cBn/MXByyzSpZrlDtlMQppVrl8hLfnN2alMUPWrTBqYHpkV
IZpqcexhxLrL2yb8mYpW05Y8/WmTE0cXJASmRCkmqnrcRIAE+JTdLSP9C4lX
wWkT0HPAt6zv9T0nA1XJ+cEjQYAeTeb/l2kFrwTvBVWFQzbkdz0OTaBj2YCt
2lIKvzoCS2ylCtnwj5yUn0Y89JiJO+LtFphngQ2UqgRJRKtsdN4UdpJ4JvBp
qTORw4DnqEyQP1d0r09vwOXKGYk3/edNbO7nFFuX46ligdqGWSaf6Sj+e7ow
FhxjF22cEX8zdIz0pq8W8okwOVk/n9FXejHKDpAE21PW9PyczHNGCnlZrQyP
7IiaLo/VhXr7URrMDpMfqvkl/aZuivTLh467Mm7rf6cl/4MzSKWVoh/13gWf
KYjIvwkqx3HRqSILoKukjO2mwM+OWJWFPdijYQwUgQNDLv/fKkwsYGjH4nDG
Wn/k
=f0yM
-----END PGP SIGNATURE-----
```