Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

S . G . D . S . N
Agence nationale de la sécurité des systèmes d'information
CERT-FR

Paris, le 10 février 2016
N° CERTFR-2016-AVI-055

Affaire suivie par :
CERT-FR

AVIS DU CERT-FR

Objet : Multiples vulnérabilités dans Microsoft Internet Explorer

Gestion du document

Référence	CERTFR-2016-AVI-055
Titre	Multiples vulnérabilités dans Microsoft Internet Explorer
Date de la première version	10 février 2016
Date de la dernière version	–
Source(s)	Bulletin de sécurité Microsoft MS16-009 du 09 février 2016 Bulletin de sécurité Microsoft MS16-022 du 09 février 2016 Bulletin de sécurité Adobe APSB16-04 du 09 février 2016
Pièce(s) jointe(s)	Aucune

TAB. 1 – *Gestion du document*

Une gestion de version détaillée se trouve à la fin de ce document.

1 - Risque(s)

- exécution de code arbitraire à distance
- contournement de la politique de sécurité
- atteinte à la confidentialité des données
- élévation de privilèges

2 - Systèmes affectés

- Microsoft Internet Explorer 9 pour Windows Vista SP2
- Microsoft Internet Explorer 9 pour Windows Server 2008 SP2
- Microsoft Internet Explorer 10 pour Windows Server 2012
- Microsoft Internet Explorer 11 pour Windows 7 SP1
- Microsoft Internet Explorer 11 pour Windows 8.1
- Microsoft Internet Explorer 11 pour Windows Server 2008 R2
- Microsoft Internet Explorer 11 pour Windows Server 2012 R2
- Microsoft Internet Explorer 11 pour Windows RT 8.1
- Microsoft Internet Explorer 11 pour Windows 10
- Adobe Flash Player pour Windows Internet Explorer 10 et 11 sur Windows 8.1 et 10, Windows Server 2012 et 2012 R2, et Windows RT 8.1

3 - Résumé

De multiples vulnérabilités ont été corrigées dans *Microsoft Internet Explorer*. Certaines d'entre elles permettent à un attaquant de provoquer une exécution de code arbitraire à distance, un contournement de la politique de sécurité et une atteinte à la confidentialité des données.

4 - Solution

Se référer au bulletin de sécurité de l'éditeur pour l'obtention des correctifs (cf. section Documentation).

5 - Documentation

- Bulletin de sécurité Microsoft MS16-009 du 09 février 2016
  https://technet.microsoft.com/en-us/library/security/ms16-009
- Bulletin de sécurité Microsoft MS16-022 du 09 février 2016
  https://technet.microsoft.com/en-us/library/security/ms16-022
- Bulletin de sécurité Adobe APSB16-04 du 09 février 2016
  https://helpx.adobe.com/security/products/flash-player/apsb16-04.html
- Référence CVE CVE-2016-0041
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0041
- Référence CVE CVE-2016-0059
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0059
- Référence CVE CVE-2016-0060
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0060
- Référence CVE CVE-2016-0061
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0061
- Référence CVE CVE-2016-0062
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0062
- Référence CVE CVE-2016-0063
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0063
- Référence CVE CVE-2016-0064
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0064
- Référence CVE CVE-2016-0067
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0067
- Référence CVE CVE-2016-0068
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0068
- Référence CVE CVE-2016-0069
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0069
- Référence CVE CVE-2016-0071
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0071
- Référence CVE CVE-2016-0072
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0072
- Référence CVE CVE-2016-0077
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0077
- Référence CVE CVE-2016-0964
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0964
- Référence CVE CVE-2016-0965
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0965
- Référence CVE CVE-2016-0966
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0966
- Référence CVE CVE-2016-0967
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0967
- Référence CVE CVE-2016-0968
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0968

- Référence CVE CVE-2016-0969
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0969
- Référence CVE CVE-2016-0970
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0970
- Référence CVE CVE-2016-0971
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0971
- Référence CVE CVE-2016-0972
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0972
- Référence CVE CVE-2016-0973
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0973
- Référence CVE CVE-2016-0974
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0974
- Référence CVE CVE-2016-0975
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0975
- Référence CVE CVE-2016-0976
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0976
- Référence CVE CVE-2016-0977
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0977
- Référence CVE CVE-2016-0978
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0978
- Référence CVE CVE-2016-0979
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0979
- Référence CVE CVE-2016-0980
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0980
- Référence CVE CVE-2016-0981
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0981
- Référence CVE CVE-2016-0982
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0982
- Référence CVE CVE-2016-0983
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0983
- Référence CVE CVE-2016-0984
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0984
- Référence CVE CVE-2016-0985
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0985

Gestion détaillée du document

10 février 2016 version initiale.