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 02 mai 2017
N° CERTFR-2017-AVI-136

Affaire suivie par :
CERT-FR

AVIS DU CERT-FR

Objet : Vulnérabilité dans les micrologiciels Intel

Gestion du document

Référence	CERTFR-2017-AVI-136
Titre	Vulnérabilité dans les micrologiciels Intel
Date de la première version	02 mai 2017
Date de la dernière version	–
Source(s)	Bulletin de sécurité Intel INTEL-SA-00075 du 01 mai 2017
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
- élévation de privilèges

2 - Systèmes affectés

- Intel Active Management Technology (AMT), Intel Standard Manageability (ISM), et Intel Small Business Technology versions 6.x antérieures à 6.2.61.3535
- Intel Active Management Technology (AMT), Intel Standard Manageability (ISM), et Intel Small Business Technology versions 7.x antérieures à 7.1.91.3272
- Intel Active Management Technology (AMT), Intel Standard Manageability (ISM), et Intel Small Business Technology versions 8.x antérieures à 8.1.71.3608
- Intel Active Management Technology (AMT), Intel Standard Manageability (ISM), et Intel Small Business Technology versions 9.0.x et 9.1.x antérieures à 9.1.41.3024
- Intel Active Management Technology (AMT), Intel Standard Manageability (ISM), et Intel Small Business Technology versions 9.5.x antérieures à 9.5.61.3012
- Intel Active Management Technology (AMT), Intel Standard Manageability (ISM), et Intel Small Business Technology versions 10.x antérieures à 10.0.55.3000
- Intel Active Management Technology (AMT), Intel Standard Manageability (ISM), et Intel Small Business Technology versions 11.0.x antérieures à 11.0.25.3001

– Intel Active Management Technology (AMT), Intel Standard Manageability (ISM), et Intel Small Business Technology versions 11.5.x et 11.6.x antérieures à 11.6.27.3264

3 - Résumé

Une vulnérabilité a été corrigée dans *les micrologiciels Intel*. Elle permet à un attaquant de provoquer une exécution de code arbitraire à distance et une élévation de privilèges.

La vulnérabilité impacte le composant Advanced Management Technology (AMT) des micro-logiciels Intel vulnérables. AMT est une technologie Intel permettant d'administrer (surveiller la disponibilité, mettre à jour, redémarrer, etc.) des systèmes à distance via un canal de communication séparé du système d'exploitation. Les produits ISM (Intel Standard Manageability) et SBT (Small Business Technology) permettent d'accéder à un sous ensemble des fonctionnalités AMT.

Les produits AMT et ISM exposent la fonctionnalité vulnérable sur le réseau et permettraient à un attaquant la prise de contrôle à distance d'un système sans authentification au préalable.

D'autre part, un attaquant ayant un accès local au système vulnérable pourrait élever ses privilèges en exploitant cette vulnérabilité.

Intel a mis à disposition un guide permettant d'identifier si un système est vulnérable [1] ainsi qu'une procédure proposant des contre-mesures lorsque la mise à jour n'est pas disponible pour le composant impacté [2].

4 - Solution

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

5 - Documentation

– 1 Guide Intel
https://communities.intel.com/docs/DOC-5693
– 2 Contre-mesures Intel
https://downloadcenter.intel.com/download/26754
– Bulletin de sécurité Intel INTEL-SA-00075 du 01 mai 2017
https://security-center.intel.com/advisory.aspx?intelid=INTEL-SA-00075&languageid=en-fr
– Référence CVE CVE-2017-5689
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-5689

Gestion détaillée du document

02 mai 2017 version initiale.