Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

S . G . D . S . N
Agence nationale de la sécurité des systèmes d'information
CERTA

Paris, le 19 décembre 2011
N° CERTA-2011-AVI-708

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Vulnérabilité dans Intel TXT (solution de sécurité de processeurs Intel) SINIT

Gestion du document

Référence	CERTA-2011-AVI-708
Titre	Vulnérabilité dans Intel TXT (solution de sécurité de processeurs Intel) SINIT
Date de la première version	19 décembre 2011
Date de la dernière version	–
Source(s)	Bulletin de sécurité Intel du 05 décembre 2011
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

Élévation de privilèges.

2 Systèmes affectés

Processeurs Intel avec l'extension Intel *Trusted Execution Technology* (consultez le bulletin de sécurité Intel cité dans la section Documentation pour une liste exhaustive des processeurs concernés).

3 Résumé

Une vulnérabilité présente dans Intel *Trusted Execution Technology* (Intel TXT) SINIT *Authenticated Code Modules* (ACM) permet à une personne malveillante de contourner la solution de sécurité Intel TXT.

4 Description

Une vulnérabilité de type dépassement de tampon (*buffer overflow*) est présente dans Intel *Trusted Execution Technology* SINIT *Authenticated Code Modules* (ACM).

Intel *Trusted Execution Technology* (Intel TXT) est une solution de sécurité matérielle qui vise à fournir un mécanisme de protection contre les attaques logicielles en vérifiant le comportement de certains composants d'une machine au démarrage.

Lorsque le lancement mesuré (*measured launch*) de Intel TXT est effectué en utilisant SINIT ACM, la vulnérabilité peut être exploitée pour contourner Intel TXT.

5 Solution

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

6 Documentation

– Bulletin de sécurité Intel du 05 décembre 2011 :
http://security-center.intel.com/advisory.aspx?intelid=INTEL-SA-00030&languageid=en-fr

Gestion détaillée du document

19 décembre 2011 version initiale.