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 29 juin 2016
N° CERTFR-2016-AVI-222

**Affaire suivie par :**
CERT-FR

# AVIS DU CERT-FR

**Objet : Multiples vulnérabilités dans les produits Symantec**

## Gestion du document

| | |
|---|---|
| Référence | CERTFR-2016-AVI-222 |
| Titre | Multiples vulnérabilités dans les produits Symantec |
| Date de la première version | 29 juin 2016 |
| Date de la dernière version | – |
| Source(s) | Bulletin de sécurité Symantec SYM16-010 du 28 juin 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

## 2 - Systèmes affectés

- Symantec Advanced Threat Protection (ATP) sans le dernier correctif de sécurité
- Symantec Data Center Server (SDCS:SA) version 6.6 MP1 sans le dernier correctif de sécurité
- Symantec Data Center Server (SDCS:SA) version 6.5 MP1 sans le dernier correctif de sécurité
- Symantec Critical System Protection (SCSP) version 5.2.9 MP6 sans le dernier correctif de sécurité
- Symantec Embedded Systems Critical System Protection (SES:CSP) version 1.0 MP5 sans le dernier correctif de sécurité
- Symantec Embedded Systems Critical System Protection (SES:CSP) version 6.5.0 MP1 sans le dernier correctif de sécurité
- Symantec Web Security .Cloud
- Symantec Email Security Server .Cloud (ESS)
- Symantec Web Gateway
- Symantec Endpoint Protection (SEP) versions antérieures à SEP 12.1 RU6 MP5
- Symantec Endpoint Protection pour Mac (SEP pour Mac) versions 12.1.6 MP4 et antérieures sans le dernier correctif de sécurité
- Symantec Endpoint Protection pour Linux (SEP pour Linux) versions antérieures à 12.1 RU6 MP5
- Symantec Protection Engine (SPE) versions antérieures à SPE 7.0.5 HF01

- Symantec Protection Engine (SPE) versions 7.5.4 antérieures à SPE 7.5.4 HF01
- Symantec Protection Engine (SPE) versions 7.5.3 antérieures à SPE 7.5.3 HF03
- Symantec Protection Engine (SPE) versions 7.8 antérieures à SPE 7.8.0 HF01
- Symantec Protection for SharePoint Servers (SPSS) versions 6.03 à 6.05 sans le correctif de sécurité SPSS_6.0.3_To_6.0.5_HF
- Symantec Protection for SharePoint Servers (SPSS) version 6.0.6 sans le correctif de sécurité SSPSS_6.0.6_HF_1.6
- Symantec Mail Security for Microsoft Exchange (SMSMSE) versions 7.0.4 et antérieures sans le correctif de sécurité SMSMSE_7.0_3966002_HF1.1
- Symantec Mail Security for Microsoft Exchange (SMSMSE) versions 7.5.4 et antérieures sans le correctif de sécurité SMSMSE_7.5_3966008_VHF1.2
- Symantec Mail Security for Domino (SMSDOM) versions 8.0.9 et antérieures sans le correctif de sécurité SMSDOM_8.0.9_HF1.1
- Symantec Mail Security for Domino (SMSDOM) versions 8.1.3 et antérieures sans le correctif de sécurité SMSDOM_8.1.3_HF1.2
- Symantec CSAPI versions antérieures à 10.0.4 HF01
- Symantec Message Gateway (SMG) versions antérieures à 10.6.1-4
- Symantec Message Gateway for Service Providers (SMG-SP) version 10.6 sans le correctif de sécurité 253
- Symantec Message Gateway for Service Providers (SMG-SP) version 10.5 sans le correctif de sécurité 254
- Norton AntiVirus versions antérieures à 22.7
- Norton Security versions antérieures à 22.7
- Norton Security with Backup versions antérieures à 22.7
- Norton Internet Security versions antérieures à 22.7
- Norton 360 versions antérieures à 22.7
- Norton Security pour Mac versions antérieures à 13.0.2
- Norton Power Eraser (NPE) versions antérieures à 5.1
- Norton Bootable Removal Tool (NBRT) versions antérieures à 2016.1

# 3 - Résumé

De multiples vulnérabilités ont été corrigées dans *les produits Symantec*. Elles permettent à un attaquant de provoquer une exécution de code arbitraire à distance.

# 4 - Solution

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

# 5 - Documentation

- Bulletin de sécurité Symantec SYM16-010 du 28 juin 2016
  https://www.symantec.com/security_response/securityupdates/detail.jsp?fid=security_advisory&pvid=security_advisory&yea
- Blog Google Project Zero
  https://googleprojectzero.blogspot.fr/2016/06/how-to-compromise-enterprise-endpoint.html
- Référence CVE CVE-2016-2207
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-2207
- Référence CVE CVE-2016-2209
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-2209
- Référence CVE CVE-2016-2210
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-2210
- Référence CVE CVE-2016-2211
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-2211
- Référence CVE CVE-2016-3644
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-3644
- Référence CVE CVE-2016-3645
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-3645

# Gestion détaillée du document

**29 juin 2016** version initiale.

| | |
|---|---|
| Conditions d'utilisation de ce document : | http://cert.ssi.gouv.fr/cert-fr/apropos.html |
| Dernière version de ce document : | http://cert.ssi.gouv.fr/site/CERTFR-2016-AVI-222 |