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 08 octobre 2014
N° CERTFR-2014-AVI-409

Affaire suivie par :
CERT-FR

AVIS DU CERT-FR

Objet : Multiples vulnérabilités dans Huawei

Gestion du document

Référence	CERTFR-2014-AVI-409
Titre	Multiples vulnérabilités dans Huawei
Date de la première version	08 octobre 2014
Date de la dernière version	–
Source(s)	Bulletin de sécurité Huawei Huawei-SA-20141008-OpenSSL du 08 octobre 2014
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
- déni de service à distance
- contournement de la politique de sécurité
- atteinte à l'intégrité des données
- atteinte à la confidentialité des données

2 - Systèmes affectés

- Huawei AP5010DN-AGN versions antérieures à V200R005C10
- Huawei eSDK Solution versions antérieures à V100R003C30SPC100
- Huawei eSight UC&C versions antérieures à V100R001C01SPC303
- Huawei eSight UC&C versions antérieures à V100R001C20SPC306
- Huawei eSight UC&C versions antérieures à V300R002C00SPC200
- Huawei FusionAccess versions antérieures à V100R005C20
- Huawei HUAWEI S12700 versions antérieures à V200R006C00SPC300
- Huawei OceanStor S6800T versions antérieures à V100R005C30SPC300
- Huawei OceanStor S6800T versions antérieures à V200R002C20SPC100
- Huawei OceanStor S6800T versions antérieures à V200R002C00SPC400
- Huawei OceanStor S2600T versions antérieures à V100R005C30SPC300
- Huawei OceanStor S2600T versions antérieures à V200R002C00SPC400

- Huawei OceanStor S2600T versions antérieures à V100R005C30SPC300
- Huawei OceanStor S2600T versions antérieures à V200R002C20SPC100
- Huawei OceanStor S2600T versions antérieures à V200R002C00SPC400
- Huawei OceanStor S5500T versions antérieures à V100R005C30SPC300
- Huawei OceanStor S5500T versions antérieures à V200R002C20SPC100
- Huawei OceanStor 18800 versions antérieures à V100R001C00SPC300
- Huawei OceanStor S5600T versions antérieures à V100R005C30SPC300
- Huawei OceanStor S5600T versions antérieures à V200R002C20SPC100
- Huawei OceanStor S5600T versions antérieures à V200R002C00SPC400
- Huawei OceanStor S5800T versions antérieures à V100R005C30SPC300
- Huawei OceanStor S5800T versions antérieures à V200R002C20
- Huawei OceanStor S5800T versions antérieures à V200R002C00SPC400
- Huawei OceanStor 18800F versions antérieures à V100R001C00SPC300
- Huawei OceanStor 18500 versions antérieures à V100R001C00SPC300
- Huawei OceanStor 6800 V3 versions antérieures à V300R001C10SPC100
- Huawei OceanStor N8500 versions antérieures à V200R001C09SPC502
- Huawei V200R001C91SPC200 versions antérieures à V200R001C91SPC202
- Huawei OceanStor HVS88T versions antérieures à V100R001C00SPC300
- Huawei OceanStor HVS85T versions antérieures à V100R001C00SPC300
- Huawei OceanStor S2200T versions antérieures à V100R005C30SPC300
- Huawei OceanStor S2900 versions antérieures à V100R005C30SPC300
- Huawei OceanStor S3900 versions antérieures à V100R005C30SPC300
- Huawei OceanStor S6900 versions antérieures à V100R005C30SPC300
- Huawei OceanStor Dorado2100 versions antérieures à V100R001C00SPCa00
- Huawei OceanStor Dorado2100G2 versions antérieures à V100R001C00SPCa00
- Huawei OceanStor Dorado5100 versions antérieures à V100R001C00SPCa00
- Huawei RSE6500 versions antérieures à V100R001C00SPC200
- Huawei S7700 versions antérieures à V200R006C00SPC300
- Huawei S3300 versions antérieures à V100R006HP0011
- Huawei SoftCo versions antérieures à V200R001C01SPC500
- Huawei SmartCDN versions antérieures à V100R001C05SPC600T
- Huawei TSM versions antérieures à TSM V100R002C07SPC224
- Huawei TSM versions antérieures à Policy Center V100R003C10
- Huawei USG9560 versions antérieures à USG9560 V300R001C01SPH303
- Huawei USG9500 versions antérieures à V300R001C01SPH303
- Huawei USG9300 versions antérieures à USG9500 V300R001C01SPH303

3 - Résumé

De multiples vulnérabilités ont été corrigées dans *Huawei*. Certaines d'entre elles permettent à un attaquant de provoquer une exécution de code arbitraire à distance, un déni de service à distance et un contournement de la politique de sécurité.

4 - Solution

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

5 - Documentation

- Bulletin de sécurité Huawei Huawei-SA-20141008-OpenSSL du 08 octobre 2014
  http://www.huawei.com/en/security/psirt/security-bulletins/security-advisories/hw-372998.htm

- Référence CVE CVE-2014-3505
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3505
- Référence CVE CVE-2014-3506
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3506
- Référence CVE CVE-2014-3507
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3507
- Référence CVE CVE-2014-3508
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3508
- Référence CVE CVE-2014-3509
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3509
- Référence CVE CVE-2014-3510
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3510
- Référence CVE CVE-2014-3511
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3511
- Référence CVE CVE-2014-3512
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3512
- Référence CVE CVE-2014-5139
  http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-5139

Gestion détaillée du document

08 octobre 2014 version initiale.