

Affaire suivie par :
CERTA

BULLETIN D'ALERTE DU CERTA

Objet : Vulnérabilité de HelixPlayer et RealPlayer

Conditions d'utilisation de ce document : <http://www.certa.ssi.gouv.fr/certa/apropos.html>
Dernière version de ce document : <http://www.certa.ssi.gouv.fr/site/CERTA-2005-ALE-011>

Gestion du document

Référence	CERTA-2005-ALE-011-002
Titre	Vulnérabilité de HelixPlayer et RealPlayer
Date de la première version	27 septembre 2005
Date de la dernière version	10 octobre 2005
Source(s)	Bulletin de sécurité Secunia SA16954 du 27 septembre 2005
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

Exécution de code arbitraire à distance.

2 Systèmes affectés

- HelixPlayer versions 1.0.5.757 et antérieures ;
- RealPlayer versions 10.0.5.756 (gold) et antérieures.

3 Résumé

Une vulnérabilité dans HelixPlayer et RealPlayer permet à un utilisateur distant d'exécuter du code arbitraire.

4 Description

Une vulnérabilité dans la fonction d'affichage du message *invalid-handle error* permet à un utilisateur distant mal intentionné d'exécuter du code arbitraire par le biais d'un site web mettant à disposition un fichier avec l'extension `.rp` ou `.rt` malicieusement constitué. Remarque : L'exploitation de cette vulnérabilité n'est possible que sur les systèmes GNU/Linux.

5 Contournement provisoire

Ne pas utiliser RealPlayer ou HelixPlayer pour visionner des fichiers d'extensions `.rp` ou `.rt`.

6 Solution

Se référer aux bulletins de sécurité des éditeurs pour appliquer les correctifs appropriés (cf. Documentation).

7 Documentation

- Site Internet de RealPlayer :
<http://www.real.com/player/>
- Site Internet de HelixPlayer :
<http://player.helixcommunity.org>
- Bulletin de sécurité Secunia SA16954 du 27 septembre 2005 :
<http://secunia.com/advisories/16954/>
- Bulletin de sécurité RedHat RHSA-2005:788 du 27 septembre 2005 :
<http://rhn.redhat.com/errata/RHSA-2005-788.html>
- Mises à jour de sécurité Fedora Core 3 et Fedora Core 4 pour HelixPlayer du 27 septembre 2005 :
<http://download.fedora.redhat.com/pub/fedora/linux/core/updates/3/>
<http://download.fedora.redhat.com/pub/fedora/linux/core/updates/4/>
- Bulletin de sécurité Debian DSA-826 du 29 septembre 2005 :
<http://www.debian.org/security/2005/dsa-826>
- Bulletin de sécurité Gentoo GLSA-200510-07 du 07 octobre 2005 :
<http://www.gentoo.org/security/en/glsa/glsa-200510-07.xml>
- Référence CVE CAN-2005-2710 :
<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-2710>

Gestion détaillée du document

27 septembre 2005 version initiale.

28 septembre 2005 ajout d'une section Solution, des sites Internet de RealPlayer et HelixPlayer, des références aux bulletins de sécurité Fedora et RedHat RHSA-2005:788 et de la référence CVE CAN-2005-2710.

10 octobre 2005 ajout des références aux bulletins de Debian et Gentoo.