



Cisco Security Notice : BugTraq への回答 - HSRP の問題

目次

要約
詳細情報
シスコのセキュリティ手順

要約

このドキュメントは、シスコのお客様用のパブリック フォーラムに掲載された、製品セキュリティの潜在的な脆弱性の問題に対するシスコの回答へのアクセスを容易にするために提供されています。これは、シスコがこれらの各問題を実際の製品セキュリティの脆弱性として認識していることを意味するものではありません。この通知は「現状のまま」で提供されるものであり、いかなる約束または保証を意味するものでもありません。このページの情報またはこのページからリンクされている資料は、お客様ご自身の責任においてご利用ください。シスコは、いつでも予告なしに、このページを変更またはアップデートする権利を留保します。

詳細情報

元のレポート : <http://www.securityfocus.com/archive/1/182008>

シスコは、次の内容を回答しました。

この回答も <http://www.securityfocus.com/archive/1/184814> にアーカイブされています。

To: BugTraq
Subject: Re: Cisco HSRP Weakness/DoS
Date: May 16 2001 7:42AM
Author: Damir Rajnovic <gaus@cisco.com>
Message-ID: <4.3.2.7.2.20010516074146.023c1d50@144.254.74.238>

Hello,

Seems that this mail has been lost again.

Gaus

My previous mail seems to be lost due to the mail server problems
so here is the response again.

In response to this mail sent by bashis on Bugtraq:

At 19:57 03/05/2001 +0200, bashis wrote:
>I was playing with Cisco's HSRP (Hot Standby Routing Protocol),
>and there is a (major) weakness in that protocol that allow
>any host in a LAN segment to make a HSRP DoS.
[truncated, see <http://www.securityfocus.com/archive/1/182008>]

We can confirm that described vulnerability is present in the HSRP
and, at the present time, there is no workaround for it.

Cisco is deliberating usage of IP authenticated header for HSRP
and VRRP (Virtual Router Redundancy Protocol, RFC2338) in the future
releases of IOS.

However, there are some other factors that must be considered in
this context:

- this vulnerability can be exploited only from the local segment
(not over the Internet),
- the same effect, denial of service, can be produced by using ARP,
which can not be protected in any way

The last issue is especially important since it may cause a false sense of security if user is using a hardened version the protocol (whichever protocol). Even by using VRRP and ESP+AH option, an attacker can still disrupt the network by using ARP.

Regards,

Gaus

=====

Damir Rajnovic <psirt@cisco.com>, PSIRT Incident Manager, Cisco Systems
<http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html>
Phone: +44 7715 546 033
4 The Square, Stockley Park, Uxbridge, MIDDLESEX UB11 1BN, GB

=====

There is no insolvable problems. Question remains: can you accept the solution?

シスコのセキュリティ手順

シスコ製品のセキュリティの脆弱性に関するレポート、セキュリティ障害に対する支援、およびシスコからのセキュリティ情報を受信するための登録に関するすべての情報は、シスコのワールドワイド ウェブサイト

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html から入手できます。この情報には、シスコのセキュリティ通知に関して、報道機関が問い合わせる場合の説明も含まれています。すべての Cisco セキュリティ アドバイザリは、<http://www.cisco.com/go/psirt> から入手できます。

1992 - 2014 Cisco Systems, Inc. All rights reserved.

Updated: 2004 年 10 月 13 日

Document ID: 60007

http://www.cisco.com/cisco/web/support/JP/106/1066/1066564_cisco-sn-20010516-hsrp-j.html
