strongSwan - Bug #2088

Cisco Unity vendor ID polymorphism

23.08.2016 14:52 - Pavel Kankovsky

Status:	Closed	**Start date:**	23.08.2016
Priority:	Normal	**Due date:**	
Assignee:	Tobias Brunner	**Estimated time:**	0.00 hour
Category:	interoperability		
Target version:	5.5.1		
Affected version:	5.4.0	**Resolution:**	Fixed

Description

I wanted to connect strongSwan (as an initiator) to FortiGate (responder) using IKEv1. FortiGate was supposed to provide the configuration for split tunneling, presumably using Cisco Unity extensions of mode config. It went as follows (when I had overcome other unrelated problems...):

1. strongSwan sent the Unity VID
2. FortiGate did **NOT** send the Unity VID
3. strongSwan sent a mode config request CPRQ (ADDR DNS)
4. FortiGate sent a mode config reponse CPRP (ADDR DNS DNS)

Split tunneling configuration was nowhere to be seen.

I did some experimental brain surgery on strongSwan to make it always assume Unity extensions are supported and (voila!) it asked for additional mode config attributes and got an expected and correct response:

3. strongSwan sent CPRQ (ADDR DNS U_SPLITINC U_LOCALLAN)
4. FortiGate sent CPRP (ADDR DNS DNS **U_SPLITINC**)

It turns out FortiGate did not send the Unity VID (as recognized by strongSwan) but it sent an unrecognized vendor ID 12:f5:f2:8c:45:71:68:a9:70:2d:9f:e2:74:cc:02:04 having two very interesting properties:

(a) FortiGate sent it if and only if strongSwan had sent the Unity VID first (cisco_unity = yes).
(b) It is almost identical to the well-known Unity VID, only their two last octets differ (02:04 vs 01:00).

I did some digging and have found a few other reports of a mutant Unity VID appearing in the wild, e.g.
https://lists.openswan.org/pipermail/users/2009-September/017385.html
https://community.ubnt.com/t5/EdgeMAX/IPSec-VPN-ERL-to-Netgear/td-p/898638
https://community.sophos.com/cfs-file/__key/telligent-evolution-components-attachments/00-58-00-00-00-05-51-00/IpSec-Log.txt

Shrew Soft's implementation of IKEv1 seems to assume the last two octets of the Unity VID serve as a version number of Unity extensions e.g. 01:00 stands for 1.0 (see entries for r560 and r612 in their changelog: https://www.shrew.net/download/changelog/ike/2.2.0-release). I have not been able to found another source confirming that hypothesis but it sounds quite plausible.

I modified strongSwan to check only the first 14 octets of the Unity VID and disregard the remaining two (see the attached patch) and it is able to recognize the mutant VID sent by FortiGate and acquire the complete configuration now.

Associated revisions

Revision 17ecc104 - 24.08.2016 17:46 - Tobias Brunner

ikev1: Ignore the last two bytes of the Cisco Unity vendor ID

These seem to indicate the major and minor version of the protocol, like
e.g. for the DPD vendor ID. Some implementations seem to send versions
other than 1.0 so we just ignore these for now when checking for known
vendor IDs.

Fixes #2088.

History

#1 - 23.08.2016 16:50 - Tobias Brunner

- Tracker changed from Issue to Bug

- Category changed from ikev1 to interoperability

- Status changed from New to Feedback

- Target version set to 5.5.1

Yeah, that stuff is unstandardized and undocumented, so I guess everybody does just what others seem to be doing. You should consider using IKEv2.

The MD5 hash of "CISCO-UNITY" is actually 12:f5:f2:8c:45:71:68:a9:70:2d:9f:e2:74:cc:02:d4 that the last two bytes are changed is probably a nod to other IKEv1 extensions like DPD (RFC 3706), where the last two bytes indicate the major and minor version of the protocol. We always sent/expected it with 01:00 (already the old pluto daemon did so) as do other implementations like racoon on iOS. If there really are newer versions we could probably ignore these two bytes, but I wonder if it's problematic to blindly do so (and if we should start sending a newer version, but at least for this device that doesn't seem to be necessary).

Fix is in the *2088-unity-vendor-id* branch.

#2 - 24.08.2016 16:27 - Pavel Kankovsky

Tobias Brunner wrote:

> You should consider using IKEv2.

I would **totally** use IKEv2... if the other party were to allow that.

> If there really are newer versions we could probably ignore these two bytes, but I wonder if it's problematic to blindly do so

I, ahem, examined a copy of ancient Cisco VPN client 4.8. As far as I can tell, it does exactly that thing to recognize whether a peer is "Cisco-Unity compliant": check whether a VID is 16 bytes long and whether its first 14 bytes match, the remaining two are ignored. (BTW: They seem to handle DPD VID in a similar way.)

> (and if we should start sending a newer version, but at least for this device that doesn't seem to be necessary).

Shrew Soft seems to have tried that in 2008 (as documented by the changelog I mentioned in my original report) but reverted the change after several months because racoon (as well as many other implementations, I guess) would fail to recognize the "updated" VID. I think it would be wiser to stick to the well-known "original" VID.

#3 - 24.08.2016 17:47 - Tobias Brunner

- Status changed from Feedback to Closed

- Resolution set to Fixed

> > If there really are newer versions we could probably ignore these two bytes, but I wonder if it's problematic to blindly do so
>
> I, ahem, examined a copy of ancient Cisco VPN client 4.8. As far as I can tell, it does exactly that thing to recognize whether a peer is "Cisco-Unity compliant": check whether a VID is 16 bytes long and whether its first 14 bytes match, the remaining two are ignored. (BTW: They seem to handle DPD VID in a similar way.)

Nice :) OK, then we go with that.

> > (and if we should start sending a newer version, but at least for this device that doesn't seem to be necessary).
>
> Shrew Soft seems to have tried that in 2008 (as documented by the changelog I mentioned in my original report) but reverted the change after several months because racoon (as well as many other implementations, I guess) would fail to recognize the "updated" VID. I think it would be wiser to stick to the well-known "original" VID.

Yeah, I guess that's safer.

Files

strongswan-5.4.0-unityvid.patch	762 Bytes	23.08.2016	Pavel Kankovsky