# Vulnerability Report Confirmation - [VRF#GJI7GHCS]

Your vulnerability report has been successfully received. You may print this page for your own records. The Report Tracking ID assigned to this report is VRF#GJI7GHCS. Details of your report are listed below.

If you have any questions or require additional information, please call the CERT Hotline at +1 412-268-7090 or send email to cert@cert.org. Please reference this Report Tracking ID: VRF#GJI7GHCS.

Do not use the back button to submit another report. Click here instead.

---

## Vulnerability Report

| | |
|---|---|
| Name | Robert A Stangarone Jr |
| Organization | whataboutbob.org/exploitdevelopment.com |
| Email Address | us-cert-submission@whataboutbob.org |
| Telephone Number | 8589452613 |
| Vulnerability Description | A default configuration of the net.ipv4.conf.all.arp_ignore value to 0 on a multi-homed Linux system allows for the enumeration of configured layer 3 IP addresses at layer 2 using Address Resolution Protocol (ARP). The configured layer 3 IP addresses are not connected to the same layer 2 link on which the enumeration is be attempted. This configuration is typically associated with a condition known as “ARP flux”. This enumeration can be achieved through the use of the “arping” utility available on many Linux distributions. For this vulnerability to be exploitable, the attacker and target would have to share layer 2 connectivity. |
| Can we provide your name to the vendor? | Yes |
| Do you want to be publicly acknowledged? | Yes |
| Vendor Notification | will not notify |

| | |
|---|---|
| Status | |
| Vendor Name | several, see additional information |
| Vendor Contact Name | several |
| Vendor Contact Email | rstangarone1@gmail.com |
| Vendor Contact Telephone Number | 8589452613 |
| Vendor Tracking ID | |
| Additional Vendor Information | Redhat (CentOS,Fedora), Ubuntu, Cisco, Various implementations using the Busybox Linux distrobutions. |
| Affected System Configurations | Any Linux based system whose net.ipv4.conf.all.arp_ignore has a default value of 0.<br><br>The author has tested for the presence of this vulnerability on the following operating systems and hardware devices:<br><br>CentOS 5.5 kernel 2.6.18-194.32.1.el5<br>Fedora 14 kernel 2.6.35.6-45.fc14.i686<br>Ubuntu 10.04 kernel 2.6.32-21<br>Ubuntu 10.10 kernel 2.6.35-25-generic<br>Cisco RVL200 v1.1.7 (Jul 13 2007 11:08:56)<br>Cisco RVS4000 firmware version V1.3.2.0<br>Busybox based Embedded Linux devices v1.13.2 |
| How was this vulnerability found? | Any Linux based system whose net.ipv4.conf.all.arp_ignore has a default value of 0.<br><br>The author has tested for the presence of this vulnerability on the following operating systems and hardware devices:<br><br>CentOS 5.5 kernel 2.6.18-194.32.1.el5<br>Fedora 14 kernel 2.6.35.6-45.fc14.i686<br>Ubuntu 10.04 kernel 2.6.32-21<br>Ubuntu 10.10 kernel 2.6.35-25-generic<br>Cisco RVL200 v1.1.7 (Jul 13 2007 11:08:56)<br>Cisco RVS4000 firmware version V1.3.2.0<br>Busybox based Embedded Linux devices v1.13.2 |
| Is the vulnerability being exploited? | No |
| Is there a public exploit? | No |
| Vulnerability Impact | The complete list of impacts of exploiting this vulnerability is undefined. At a minimum it is possible to attempt to determine which hosts on the same layer 2 segment as the attacker are multi-homed, and through a brute-force approach attempt to determine one or more public or private address space values. These address space values could be useful in situations where screened subnets are in use to protect the addresses used in DMZ configurations or other protected networks. Knowledge of these addresses could be used to in attempts to circumvent layer 3 firewall ACLs where there are permissive ingress/egress rules in place. If there are multiple multi-homed systems on the same layer 2 network segment it may be possible to populate one or more hosts/device's ARP tables with incorrect layer 3/layer 2 address pairings/values. Although unproven, there may be situations where layer 2 “smurf attacks” may be possible, similar to ARP flood attacks used against network switches. |
| | https://lists.ubuntu.com/archives/kernel-bugs/2007-June/027498.html<br>https://bugs.launchpad.net/ubuntu/+source/linux/+bug/26687 |

| | |
|---|---|
| Comments | The websites state that there was a bug filed in June 2007 for this issue where the bug author suggested changing the value to “1” would be the proper default value. The bug was eventually closed as “Incomplete” without a fix being noted.<br><br>http://book.chinaunix.net/special/ebook/oreilly/Understanding_Linux_Network_Internals/0596002556/understandlni-CHP-28-SECT-4.html#understandlni-CHP-28-SECT-4<br>The website identifies the same issue for which the report is being made. |
| Attached File | |
| Date | 2011-01-29T02:33:27 |
| Report Tracking ID | VRF#GJI7GHCS |
| CERT Tracking IDs | |