Vulnerability Note VU#950576

DSL routers contain hard-coded "XXXXairocon" credentials

Original Release date: 25 8月 2015 | Last revised: 27 8月 2015

Overview

DSL routers by ASUS, DIGICOM, Observa Telecom, Philippine Long Distance Telephone (PLDT), and ZTE contain hard-coded "`XXXXairocon`" credentials

Description

CWE-798: Use of Hard-coded Credentials

DSL routers, including the ASUS DSL-N12E, DIGICOM DG-5524T, Observa Telecom RTA01N, Philippine Long Distance Telephone (PLDT) SpeedSurf 504AN and Kasda KW58293, and ZTE ZXV10 W300 contain hard-coded credentials that are useable in the telnet service on the device. In the ASUS, DIGICOM, Observa Telecom, and ZTE devices, the username is "`admin`," in the PLDT devices, the user name is "`adminpldt`," and in all affected devices, the password is "`XXXXairocon`" where "`XXXX`" is the last four characters of the device's MAC address. The MAC address may be obtainable over SNMP with community string `public`.

The vulnerability was previously disclosed in VU#228886 and assigned CVE-2014-0329 for ZTE ZXV10 W300, but it was not known at the time that the same vulnerability affected products published by other vendors. The Observa Telecom RTA01N was previously disclosed on the Full Disclosure mailing list.

Impact

A remote attacker may utilize these credentials to gain administrator access to the device.

Solution

The CERT/CC is currently unaware of a practical solution to this problem and recommends the following workaround:

Restrict access

Enable firewall rules so the telnet service of the device is not accessible to untrusted sources. Enable firewall rules that block SNMP on the device.

Vendor Information (Learn More)

Vendor	Status	Date Notified	Date Updated
AsusTek Computer Inc.	Affected	04 May 2015	25 Aug 2015
DIGICOM (HK)	Affected	-	25 Aug 2015
Observa Telecom	Affected	-	25 Aug 2015
Philippine Long Distance Telephone	Affected	02 Jun 2015	27 Aug 2015
ZTE Corporation	Affected	03 Dec 2013	25 Aug 2015

If you are a vendor and your product is affected, let us know.

CVSS Metrics (Learn More)

Group	Score	Vector
Base	9.3	AV:N/AC:M/Au:N/C:C/I:C/A:C
Temporal	8.0	E:POC/RL:U/RC:UR
Environmental	6.0	CDP:ND/TD:M/CR:ND/IR:ND/AR:ND

References

- http://seclists.org/fulldisclosure/2015/May/129
- https://www.kb.cert.org/vuls/id/228886
- https://www.asus.com/Networking/DSLN12E/
- http://www.digicom.com.hk/index.php?section=products&action=details&id=156#.VdzlTpcuzl0
- http://www.movistar.es/particulares/atencion-cliente/internet/adsl/equipamiento-adsl/routers/router-adsl-observa-rta01n-v2/

Credit

Thanks to Walter Mostosi for reporting the issue affecting ASUS devices, Naresh LamGarde for DIGICOM devices, and to Eskie Cirrus James Maquilang for PLDT devices. Thanks again to Cesar Neira for reporting the issue in ZTE devices, and to Jose Antonio Rodriguez Garcia for disclosing the Observa Telecom vulnerability to Full Disclosure.

This document was written by Joel Land and Garret Wassermann.

Other Information

CVE IDs:	Unknown
Date Public:	25 8月 2015
Date First Published:	25 8月 2015
Date Last Updated:	27 8月 2015
Document Revision:	18

Feedback

If you have feedback, comments, or additional information about this vulnerability, please send us email.