New issue

Jump to bottom

NULL Pointer Exception when handling ipDefaultTTL #474

Open **menglong2234** opened this issue 26 days ago · 5 comments

Assignees 

menglong2234 commented 26 days ago • edited

`handle_ipDefaultTTL()` in `agent/mibgroup/ip-mib/ip_scalars.c` in Net-SNMP from 5.8 to latest(5.9.3) version has a NULL Pointer Exception bug that can be used by an unauthenticated attacker to remotely cause the instance to crash via a crafted UDP packet, resulting in Denial of Service. The PoC is here.

After sending an SNMPSET packet with a varlist [1.3.6.1.2.1.4.2.0, NULL], snmpd deamon handles the packet with `handle_ipDefaultTTL()`, in which `requests->requestvb->val.integer` reference the `val` pointer that is NULL. Then snmpd deamon crashes due to segmentation fault.

To fix this vulnerability, some pre-reference check should be perfrom like `if(!requests->requestvb->val) {return SNMP_ERR_GENERR;}`.

fenner commented 26 days ago Member

Hi, menglong2234, and thank you for this bug report. However, rather than saying that it is an unauthenticated attacker, it is more appropriate to say that it is someone with write credentials - your proof of concept does nothing unless the "private" community is configured for write access.

If there is a device with the "private" community configured for write access by default, it is appropriate to file a bug report with that device vendor - that is a severe configuration error.

menglong2234 commented 26 days ago Author

I think you're right, describing it as *unauthenticated attacker* isn't accurate. For version 2c, which does not lack security validation, you need to "guess" the field to be able to do that. XD

fenner commented 26 days ago — Member

If you ask me, SNMPv1 and SNMPv2c should not be used except for experimentation in isolated networks, even for read-only use. When SET is involved, it is even more important to use the strong authentication available in SNMPv3.

menglong2234 commented 26 days ago — Author

You are right, only SNMPv3 should be used in real production environments. However the fact is there are a large number of devices deployed with v1 and v2c, and my team still used v2c directly on devices with public IPs few years ago for configuration convenience. It really shouldn't continue to be done that way haha.

👍 1

carnil commented 19 days ago

This issue has been assigned CVE-2022-44792 .

fenner self-assigned this 16 days ago

Assignees

fenner

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

3 participants