tenable Nessus

basic scan 2

Report generated by Nessus™

Wed, 24 Jul 2024 15:32:24 CEST

TABLE OF CONTENTS

Vulnerabilities by Host

Vulnerabilities by Host

192.168.50.101

0	0	1	0	0
CRITICAL	HIGH	MEDIUM	LOW	INFO

Scan Information

Start time:	Wed Jul 24 15:10:00 2024
End time:	Wed Jul 24 15:32:24 2024

Host Information

IP:	192.168.50.101
OS:	FreeBSD 14.0-CURRENT (amd64)

Vulnerabilities

97861 - Network Time Protocol (NTP) Mode 6 Scanner

Synopsis

The remote NTP server responds to mode 6 queries.

Description

The remote NTP server responds to mode 6 queries. Devices that respond to these queries have the potential to be used in NTP amplification attacks. An unauthenticated, remote attacker could potentially exploit this, via a specially crafted mode 6 query, to cause a reflected denial of service condition.

See Also

https://ntpscan.shadowserver.org

Solution

Restrict NTP mode 6 queries.

Risk Factor

Medium

CVSS v3.0 Base Score

5.8 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:L)

CVSS v2.0 Base Score

5.0 (CVSS2#AV:N/AC:L/Au:N/C:N/I:N/A:P)

Plugin Information

Published: 2017/03/21, Modified: 2018/05/07

Plugin Output

udp/123/ntp

```
  Nessus elicited the following response from the remote
  host by sending an NTP mode 6 query :

'version="ntpd 4.2.8p17@1.4004-o Wed Nov 29 06:04:45 UTC 2023 (1)",
processor="amd64", system="FreeBSD/14.0-CURRENT", leap=3, stratum=2,
precision=-24, rootdelay=42.383, rootdisp=183.276, refid=85.199.214.99,
reftime=0xea4b7c33.977f633d, clock=0xea4b7e2e.7db4bc55, peer=55921,
tc=6, mintc=3, offset=0.000000, frequency=61.578, sys_jitter=82.173085,
clk_jitter=0.000, clk_wander=0.609'
```