

Block icmp timestamp

ICMP (Internet Control Message Protocol) is one of the protocols in the IP (Internet Protocol) suite. It is used as in error reporting by all network devices. Also network and system administrators use it to troubleshoot connectivity issues in the form of ping and traceroute.

Most people are familiar with ping and the basic functionality that ICMP provides. But ICMP provides over 40 types of control messages. Two that have been known to be used in attacks are the Timestamp Request (type 13) and Timestamp Reply (type 14). ICMP type 13 and 14 are not attacked directly, rather they provide critical information that can help attack time based security algorithms. If left unchecked they can also provide other important reconnaissance information. These issues have been around, in one form or another, for over 20 years.

```
firewall-cmd --zone=public --add-icmp-block={timestamp-request,timestamp-reply} --permanent
```

```
firewall-cmd --reload
```

Quelle: <https://www.putorius.net/mitigate-icmp-timestamp-vulnerabilities.html>

andere Möglichkeit wäre noch:

<https://www.golinuxcloud.com/disable-icmp-timestamp-responses-in-linux/>

Eindeutige ID: #1130

Verfasser: n/a

Letzte Änderung: 2023-02-06 14:13