Misc infrastructure - Bug # 197: Open portmapper email needs to be clearer

Status:	New	**Priority:**	Normal
Author:	admin	**Category:**	
Created:	2021-05-29	**Assigned to:**	
Updated:	2021-05-30	**Due date:**	
Subject:	Open portmapper email needs to be clearer		

Description:

As portmapper is an unauthenticated UDP service, it can be used in DDoS reflection attacks and it is not permitted to run such a thing completely open at BitFolk. "ShadowServer scans for open portmappers":https://www.shadowserver.org/what-we-do/network-reporting/open-portmapper-report/ and when we receive a report we pass it on to the customer asking them to fix it.

Recently a customer had ignored our emails on this subject for many days, and when they did eventually get in touch for an unrelated matter they said that they thought it was an automated email that didn't require action. The email therefore needs to be improved to make it clearer that action is required.

The current email looks like this:

@From: support@bitfolk.com@
@Subject: One or more of your BitFolk VPSes has an open portmapper service@

Dear customer,

Regular security scans have detected that one or more of your BitFolk VPSes are running the portmapper service completely open to the world.

As portmapper is a UDP service it is vulnerable to being used for amplification attacks that can cause a denial of service on a third party. It is also a security risk for yourself to be leaving portmapper accessible to the world. Therefore we need you to restrict access to this service, which can typically be achieved by firewalling off port 111 UDP.

If you have no reason to be running portmapper then you may find it preferable to simply uninstall it. On Debian and Ubuntu systems it is provided by the "portmap" and/or "rpcbind" packages.

You can perform your own check against your VPS from a remote host with something like:

@rpcinfo -p YOUR-IP-ADDRESS@

If you see a response like:

<pre>
  program vers proto   port
   100000   4   tcp   111 portmapper
   100000   3   tcp   111 portmapper
   100000   2   tcp   111 portmapper
   100000   4   udp   111 portmapper
   100000   3   udp   111 portmapper
   100000   2   udp   111 portmapper
   391002   2   tcp   819 sgi_fam
</pre>

Then your portmapper is still available, but if you see:

@rpcinfo: can't contact portmapper: RPC: Remote system error - Connection refused@

Or:

@rpcinfo: can't contact portmapper: RPC: Remote system error - Connection timed out@

Then your portmapper is unavailable from this host.

For more information please see:

https://blog.centurylink.com/a-new-ddos-reflection-attack-portmapper-an-early-warning-to-the-industry/

If you have any questions, please just reply to this email to open a support ticket.

This notice will be re-sent as we conduct future scans and continue to detect vulnerable services. Once your service is fixed you will stop receiving reports. As this is a serious problem which poses a risk to the rest of the Internet, if it is not resolved within 21 days of first detection we may have to suspend your VPS's networking:

https://tools.bitfolk.com/wiki/Vulnerability_scanning

A list of affected VPSes, relevant IP and ports and time of detection follows. If you've already fixed the problem and are still receiving this report, please check time of detection.

<pre>
"<accountname>":
    85.119.x.y:111 (UDP) detected at 2021-05-18 08:52:55 UTC
</pre>

Best regards,

Andy Smith

BitFolk Ltd

The customer has two suggestions:

> Maybe if the email subject said *IMPORTANT* or *NEEDS ACTION* then it would be more obvious that the request is more important than some automated requests that I'm used to

And:

> it is worth fronting the following paragraph:

> > This notice will be re-sent as we conduct future scans and continue to detect vulnerable services. Once your service is fixed you will stop receiving reports. As this is a serious problem which poses a risk to the rest of the Internet, if it is not resolved within 21 days of first detection we may have to suspend your VPS's networking:

> I think that would catch my attention and most other people's if it were in the first paragraph or two.

These seem like good suggestions so I propose to add "ACTION REQUIRED:" to the start of the email subject, and relocate the paragraph about consequences to near the top.

History

2021-05-29 21:11 - rr2

I think that adding â€œthat needs to be firewalledâ€• at the end of the mail will suggest that an action is required

2021-05-30 00:14 - admin

rr2 wrote:

> I think that adding â€œthat needs to be firewalledâ€• at the end of the mail will suggest that an action is required

So like where it says

> A list of affected VPSes, relevant IP and ports and time of detection follows. If you've already fixed the problem and are still receiving this report, please check time of detection.

Have

> A list of affected VPSes, relevant IP and ports and time of detection follows. All of these need to be firewalled off or shut down. If you've already fixed the problem and are still receiving this report, please check time of detection.

instead?