Give Feedback

Data Protection Vulnerability/Principle Of Least Privilege Violation

KB41044 - How to find serial number (license serial) for Pulse Secure Virtual Traffic Manager (vTM)?

11179 - Supportability of virtual traffic manager (vTM) TrafficScript

KB44330 - How to Upgrade a Cluster of Virtual Traffic Manager (vTMs) Running a Version before 17.4?

5381 - Will virtual traffic manager (vTM) v9.x support older Linux kernel versions?

13315 - What are the Supported Cipher Suites on the Pulse Secure Virtual Traffic Manager (vTM)?

KB44249 - FAQ about Pulse Secure Virtual Traffic Manager (vTM) being impacted to Bleichenbacher's Oracle (ROBOT attack)

4658 - How to change the port number for virtual traffic manager (vTM) Admin GUI?

5739 - Enable Perfect forward secrecy (PFS) on virtual traffic manager

< Back to search results

SA44790 - HTTP Request Smuggling vulnerability with Virtual Traffic Manager (vTM)

Information

Product Affected Virtual Traffic Manager (vTM)

Problem

An HTTP Request Smuggling vulnerability in Pulse Secure Virtual Traffic Manager could allow an attacker to 'smuggle' an HTTP request through an HTTP/2 header.

In particular, customers whose security relies upon the traffic manager blocking certain requests from certain backends should upgrade as soon as possible.

Customers wanting to know whether they have been impacted are advised to examine access logs on back-ends. For example (and note that other attacks are possible with other configurations), if there is a custom Trafficscript rule such as:

```
$path = http.getPath();

$ip = request.getRemoteIP();

if (string.startswithi ($path, "/admin") &&

   !string.ipmaskmatch ($ip, "1.2.3.4")) {

   http.sendResponse("403 Denied", "", "", "");
}
```

which restricts requests for /admin to only IP 1.2.3.4, then the vulnerability means requests for /admin could be allowed from IP addresses other than 1.2.3.4. The X-Cluster-Client-IP header (with the client's original IP) that vTM adds to normal requests by default is not added to the smuggled requests, and due to the nature of the vulnerability, it is possible that the X-Cluster-Client-IP header on the outer request isn't recognized by the backend as part of the outer request, hence isn't logged either. Hence, requests logged without the X-Cluster-Client-IP header that are supposed to have it may be suspicious.

Whether or not there is anything unusual in vTM's Virtual Server request logs depends on which particular header is used (attacker chosen) and if the configured log format includes logging that header.

This issue is applicable to Pulse Secure Virtual Traffic Manager. No other Pulse Secure products are currently known to be affected by this vulnerability.

CVE	CVSS Score	Product Affected
CVE-2021-31922	7.5 High 3.1#CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N	Virtual Traffic Manager

Solution

The solution for this vulnerability is to upgrade the Pulse Secure Virtual Traffic Manager to the following release:

Pulse Secure Virtual Traffic Manager	Release	Note (If any)
21.1 Pulse Secure Virtual Traffic Manager	Available Now	Cloud installation packages will be available soon. Existing customers can download the relevant cloud upgrade package now.
20.3R1 Pulse Secure Virtual Traffic Manager	Available Now	"
20.2R1 Pulse Secure Virtual Traffic Manager	Available Now	"
20.1R2 Pulse Secure Virtual Traffic Manager	Available Now	"
19.2R4 Pulse Secure Virtual Traffic Manager	Available Now	"
18.2R3 Pulse Secure Virtual Traffic Manager	Available Now	"

Document History:
May 11, 2021 - Initial advisory posted.

LEGAL DISCLAIMER

- THIS ADVISORY IS PROVIDED ON AN "AS IS" BASIS AND DOES NOT IMPLY ANY KIND OF GUARANTEE OR WARRANTY, INCLUDING THE WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. USE OF THIS INFORMATION FOUND IN THIS ADVISORY OR IN MATERIALS LINKED HERE FROM IS AT THE USER'S OWN RISK. PULSE SECURE RESERVES THE RIGHT TO CHANGE OR UPDATE THIS ADVISORY AT ANY TIME.
- A STANDALONE COPY OR PARAPHRASE OF THE TEXT OF THIS ADVISORY THAT OMITS THE DISTRIBUTION URL IS AN UNCONTROLLED COPY AND MAY OMIT IMPORTANT INFORMATION OR CONTAIN ERRORS. THE INFORMATION IN THIS ADVISORY IS INTENDED FOR END USERS OF PULSE SECURE PRODUCTS.

Workaround

This vulnerability only affects customers who are using HTTP/2. As a workaround, customers using HTTP/2 could disable HTTP/2 support in the Virtual Server > Protocol Settings.

NOTE: Customers not using HTTP/2 are not affected by this vulnerability.

Implementation

Related Links

CVSS Score 7.5 High 3.1#CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N

Risk Assessment

Acknowledgements Ivanti Team would like to thank James Kettle from PortSwigger Web Security for reporting this vulnerability.

Alert Type SA - Security Advisory

Risk Level High

Give Feedback

Yes No

Give Feedback