

Verify HTTP/2 Rapid Reset Attack Vulnerability CVE-2023-44487 on Cisco Expressways

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Background Information](#)

[Workaround for Defect CSCwh88665](#)

Introduction

This document describes how to verify and avoid HTTP/2 Rapid Reset Attack Vulnerability CVE-2023-44487 on Cisco Expressways.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

The information in this document is based on Cisco Expressway x14.X.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Background Information

On October 10, 2023, the HTTP/2 protocol-level weakness, which enables a novel distributed denial of service (DDoS) attack technique, was disclosed as CVE-2023-44487: HTTP/2 Rapid Reset.

<https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-http2-reset-d8Kf32vZ>

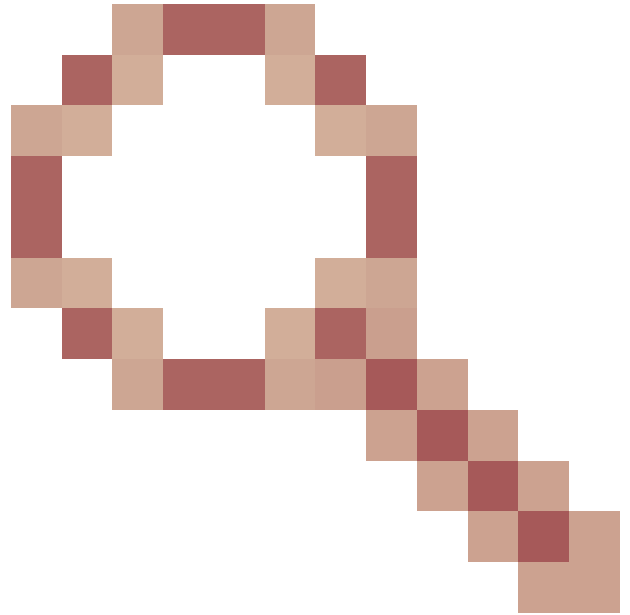
Based on the investigation performed, it is observed that Cisco Expressway is affected by this.

Here is the defect filed for evaluating the effect in Cisco Expressway. CVE-ID in discussion is currently under evaluation. Information provided in this document is briefly picked up from this Cisco Defect. Please refer below link to stay updated.

<https://bst.cloudapps.cisco.com/bugsearch/bug/CSCwh88665>

This document explains the steps to perform a workaround for this defect in the expressway to mitigate the effect of this vulnerability.

Products running x14.0 or later release with Mobile Remote Access (MRA) deployment are affected.























Workaround for Defect [CSCwh88665](#)

1. Access the expressway file system using the SCP client, (use root credentials).
Location `/tandberg/trafficserver/etc/` as shown in the image.

tandberg/trafficserver/etc/

Name

-  jabberc.reg
-  jc_srv_host.conf
-  logging.yaml
-  logging.yaml_1
-  logs_xml.config
-  parent.config
-  parent.config_17282
-  parent.config_17283
-  parent.config_17284
-  plugin.config
-  plugin.config_1
-  records.config
-  records.config_3
-  records.config_4
-  records.config_5
-  remap.config
-  remap.config_26554
-  remap.config_26555
-  remap.config_26556
-  ...

CONFIG proxy.config.http.server_ports STRING 8443:ssl

CONFIG proxy.config.http.connect_ports STRING NULL

#####

4. Modify the line:

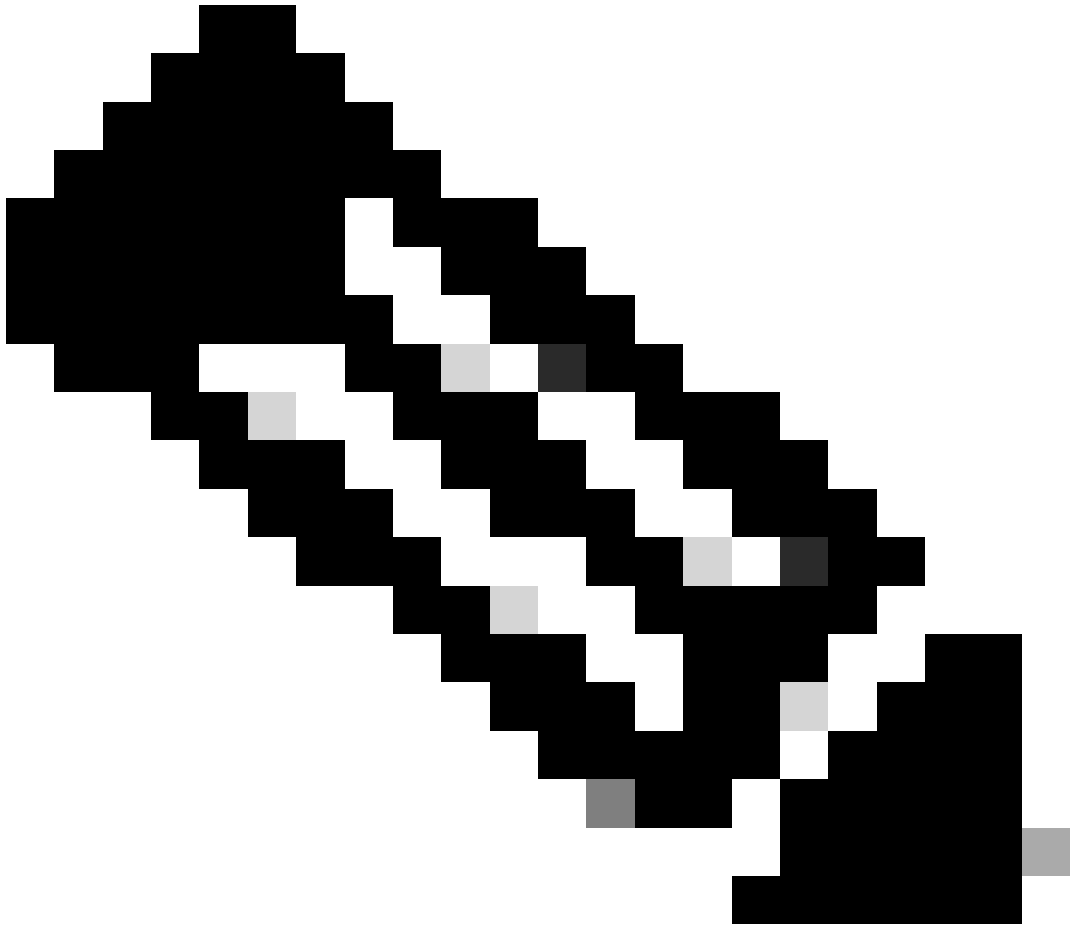
CONFIG proxy.config.http.server_ports STRING 8443:proto=http:ssl 8443:proto=http:ssl:ipv6

5. Save the file and upload it back to the same location in the expressway using WinSCP.

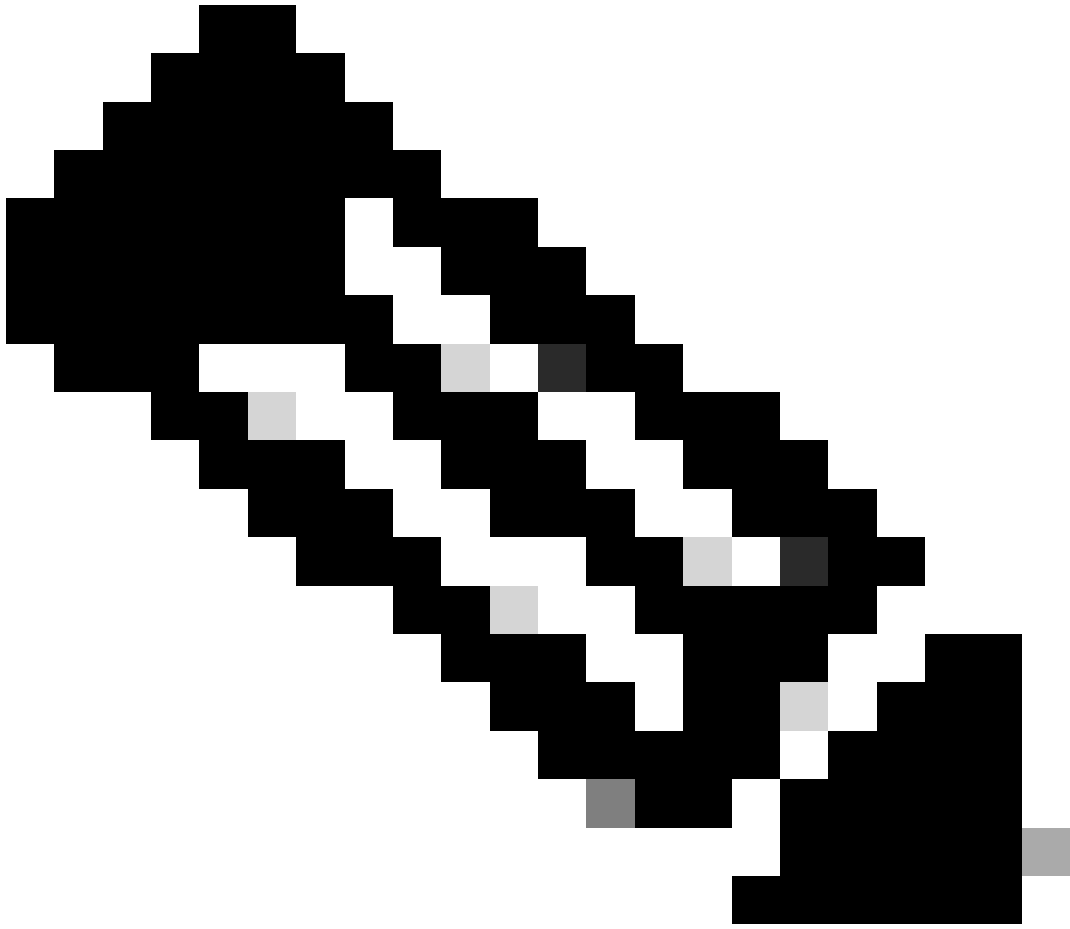
Location /tandberg/trafficserver/etc/

6. Now, login to expressway CLI using root credentials and restart “Traffic Server“ with this command /etc/init.d/trafficserver restart

```
Last login: Mon Oct 30 06:35:01 UTC 2023 from 10.65.63.238 on pts/1
~ # /etc/init.d/trafficserver restart
Stopping trafficserver
Starting trafficserver
Started trafficserver
~ # █
```



Note: System restart reverts the configuration for back to default and changes will be lost.



Note: This document is going to be further updated as more information is available.
