ACTION REQUIRED: Heroku Security notification

1 message

Salesforce <techcomms@mail.salesforce.com> Mon, Nov 7, 2022 at 15:31
Reply-to: Salesforce <reply-fe9517727265027976-2_HTML-226713488-8209301-16052@mail.salesforce.com>
To: error404forbidden56@gmail.com

HEROKU

Security Notification

At Heroku, we understand that the confidentiality, integrity, and availability of your data is vital to your business, and we take the protection of your data very seriously. We value transparency and wanted to notify you that you may be impacted by CVE-2022-3786 and CVE-2022-3602, which address the vulnerability in OpenSSL versions 3.0.0 through 3.0.6. In addition, we are providing steps you can take to determine if you were impacted, as well as steps you can take to protect your data.

What happened?

On November 1, 2022, OpenSSL, an open-source software library for applications that secure communications over computer networks, released a disclosure for CVE-2022-3786 and CVE-2022-3602 alongside a patch to address a vulnerability in versions 3.0.0 through 3.0.6. Older versions of OpenSSL are not impacted by the issues identified in CVE-2022-3786 and CVE-2022-3602.

What was the potential impact?

Maliciously-crafted TLS certificates could potentially trigger a stack overflow after certificate validation, which could enable attacks such as denial-of-service (DOS) or remote code execution (RCE). Applications that meet the following conditions may be impacted:

- Your system uses the Heroku-22 Stack
- Your system uses the Heroku Container Stack
- Your system uses Node.js

What did Heroku do to address this?

On November 1, 2022, Heroku Engineering released a new, patched stack image to the Heroku-22 Stack, and on November 4, 2022, Heroku Engineering updated all supported versions of Node.js, addressing the issues identified in CVE-2022-3786 and CVE-2022-3602 for customers that use the Heroku-22 Stack and Node.js.

What action do I need to take?

If you use the Heroku Container Stack, we do not control the stack images on your system. **As a result, you will need to take action to review your images for the presence of OpenSSL version 3.0.0 - 3.0.6. If you identify this version in your system, you must apply the patch released by OpenSSL to address the issues identified in CVE-2022-3786 and CVE-2022-3602.** In the instance that you consume binary packages provided by a distribution maintainer, please consult their documentation for further assistance.

In addition, as any applications running Node.js could potentially be impacted by CVE-2022-3786 and CVE-2022-3602, we strongly suggest that you rebuild and deploy your apps on Heroku if you are running Node.js, regardless of the stack version your application uses.

On November 3, 2022, Heroku Engineering completed the updates of the Heroku-22 Stack and relevant customer apps to address the issues identified in CVE-2022-3786 and CVE-2022-3602. As a result, if your application does not run Node.js, no further action is needed.

Heroku Data was not impacted and no further action is needed.

How can I get more information?

For more information about the issues identified in CVE-2022-3786 and CVE-2022-3602, see the FAQ document published by OpenSSL, available here. For more information on how Node.js is impacted by the issues identified in CVE-2022-3786 and CVE-2022-3602, please see the Node.js website here. For more information on how Ubuntu’s stack overflow protections, please see the Knowledge Base article Compiler Flags, available here. If you have any additional questions, please open a case with Support via the Help portal.

We sincerely regret any inconvenience you have experienced as a result of this incident and appreciate your trust in us as we continue to make your success our top priority.

Salesforce, Inc. Salesforce Tower @ 415 Mission Street, 3rd Floor, San Francisco, CA, 94105, United States
General Enquiries: 415-901-7000

This email was sent to error404forbidden56@gmail.com
Privacy Statement