Improper handling of Length parameter in erudika/scoold

0

Valid Reported on Apr 24th 2022

Description

There was no restriction on the amount of text that can be inserted into a user's name field. When the text size was large enough the service resulted in a momentary outage in our non-production environment (not high availability). An internal reproduction showed isolated disruption but no outage in our production environment.

Proof of Concept

Login account.
Visit the profile section.
Edit profile & add unlimited random input into the Name field. like
[//%3C%3E//http://www.evil.com/projectX.htm] * 10000
Save and you can see the disruption in the PoC video.

PoC

```
https://drive.google.com/file/d/18DYqGoDOdse6yLPjDb-GoqVSaFgAZkVN/view?usp=
```

Impact

When the text size is large enough the service results in a momentary outage in a production environment. That can lead to memory corruption on the server.

Occurrences

ProfileController.java L243

Chat with us

References

- huntr.dev
- HackerOne
- Blog
- Mitre

CVE
CVE-2022-1543
(Published)

Vulnerability Type
CWE-130: Improper Handling of Length Parameter Inconsistency

Severity
Critical (9.3)

Registry
Maven

Affected Version
1.49.3

Visibility
Public

Status
Fixed

Found by

Tarun Garg
@iamshooter99
pro

Fixed by

Alex Bogdanovski
@albogdano
maintainer

This report was seen 589 times.

Chat with us

We are processing your report and will contact the **erudika/scoold** team within 24 hours.
7 months ago

7 months ago

We have contacted a member of the **erudika/scoold** team and are waiting to hear back

7 months ago

Alex Bogdanovski validated this vulnerability 7 months ago

Tarun Garg has been awarded the disclosure bounty ✓

The fix bounty is now up for grabs

The researcher's credibility has increased: +7

Tarun Garg 7 months ago Researcher

@admin @maintainer @ albogdano Thank you for the bounty, Please provide for this vulnerability and Assign a CVE.

Alex Bogdanovski marked this as fixed in **1.49.4** with commit **62a0e9** 7 months ago

Alex Bogdanovski has been awarded the fix bounty ✓

This vulnerability will not receive a CVE ✗

ProfileController.java#L243 has been validated ✓

Tarun Garg 7 months ago Researcher

@admin Please assign a CVE for this vulnerability as it is public now.

Jamie Slome 7 months ago Admin

@iamshooter99 - we require the maintainer's permissions before we proceed with a CVE.

@albogdano - are you happy for us to assign and publish a CVE for this report?

Tarun Garg 7 months ago Researcher

@albogdano @maintainer @admin ?

Chat with us

Jamie Slome 7 months ago Admin

Sorted 🍰

Sign in to join this conversation