Nim's rst parser sandboxed mode allows include which can embed any local file

Critical **dom96** published **GHSA-q3vh-x957-wr75** on Jan 28

Package

NimForum (Nim)

Affected versions	Patched versions
< 2.1.0	2.2.0

docutils (Nim)

<1.6.2	None

Description

Impact

Anybody with a forum account can create a new thread/post with:

```
.. include:: /home/user/.bash_history
```

or

```
.. code::
   :file: ../forum.json
```

to access sensitive files because Nim's rst parser doesn't disallow `include` and will embed the referenced file. This can also be done silently by using NimForum's post "preview" endpoint.

Even if NimForum is running as a non-critical user, the forum.json secrets can be stolen via `.. include:: ../forum.json`.

Patches

Version 2.2.0 of NimForum includes patches for this vulnerability.

RST sandboxing is implemented in the Nim standard library, introduced by commit nim-lang/Nim@ `cb894c7` .

Workarounds

There is no workaround for this issue apart from upgrading to a newer release.

References

Version 2.2.0 announcement post on forum.nim-lang.org

Write-up on nns.ee

Severity

Critical

CVE ID

CVE-2022-23602

Weaknesses

CWE-99

Credits

nnsee