



# CVE-2017-10868

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

## Summary

<b>CVE</b>	CVE-2017-10868
<b>State</b>	PUBLIC
<b>Assigner</b>	vultures@jpcert.or.jp
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2017-12-22 14:29:00 UTC
<b>Updated</b>	2021-08-12 17:50:00 UTC
<b>Description</b>	H2O version 2.2.2 and earlier allows remote attackers to cause a denial of service in the server via specially crafted HTTP/

## Risk And Classification

**Problem Types:** CWE-20

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Dena</a>	<a href="#">H2o</a>	All	All	All	All
Application	<a href="#">H2o Project</a>	<a href="#">H2o</a>	All	All	All	All
Application	<a href="#">H2o Project</a>	<a href="#">H2o</a>	All	All	All	All

## References

Reference	Source	Link	Tags
fix crash when receiving request with invalid framing (CVE-2017-10868) · Issue #1459 · h2o/h2o · GitHub	CONFIRM	<a href="#">github.com</a>	Third
JVN#84182676: Multiple vulnerabilities in H2O	JVN	<a href="#">jvn.jp</a>	Third
CVE Program record	CVE.ORG	<a href="#">www.cve.org</a>	cano
NVD vulnerability detail	NVD	<a href="#">nvd.nist.gov</a>	cano

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

**CVE.report and Source URL Uptime Status [status.cve.report](#)**