



# CVE-2018-0608

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

## Summary

<b>CVE</b>	CVE-2018-0608
<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>	2018-06-26 14:29:00 UTC
<b>Updated</b>	2021-04-19 14:01:00 UTC
<b>Description</b>	Buffer overflow in H2O version 2.2.4 and earlier allows remote attackers to execute arbitrary code or cause a denial of serv

## Risk And Classification

**Problem Types:** CWE-119

## 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

## References

Reference	Source	Link	Tags
JVN#93226941: H2O vulnerable to buffer overflow	JVN	<a href="#">jvn.jp</a>	Third P
heap buffer overflow while trying to emit access log (CVE-2018-0608) · Issue #1775 · h2o/h2o · GitHub	MISC	<a href="#">github.com</a>	Third P
CVE Program record	CVE.ORG	<a href="#">www.cve.org</a>	canonic
NVD vulnerability detail	NVD	<a href="#">nvd.nist.gov</a>	canonic

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

[690628](#) Free Berkeley Software Distribution (FreeBSD) Security Update for h2o (ce39379f-7eb7-11e8-ab03-00bd7f19ff09)

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](#)**