



VDB-354616 · CVE-2026-1879 · GCVE-100-354616

HARVARD UNIVERSITY IQSS DATAVERSE UP TO 6.8 THEME CUSTOMIZATION /THEMEANDWIDGETS.XHTML UPLOADLOGO UNRESTRICTED UPLOAD

Summary

A vulnerability labeled as [critical](#) has been found in [Harvard University IQSS Dataverse up to 6.8](#). This impacts an unknown function of the file `/ThemeAndWidgets.xhtml` of the component `Theme Customization`. Executing a manipulation of the argument `uploadLogo` can lead to unrestricted upload. This vulnerability is handled as [CVE-2026-1879](#). The attack can be executed remotely. Additionally, an exploit exists. The affected component should be upgraded. The vendor was contacted early, responded in a very professional manner and quickly released a fixed version of the affected product.

Details

A vulnerability was found in [Harvard University IQSS Dataverse up to 6.8](#). It has been declared as critical. This vulnerability affects an unknown part of the file `/ThemeAndWidgets.xhtml` of the component `Theme Customization`. The manipulation of the argument `uploadLogo` with an unknown input leads to a unrestricted upload vulnerability. The CWE definition for the vulnerability is [CWE-434](#). The product allows the attacker to upload or transfer files of dangerous types that can be automatically processed within the product's environment. As an impact it is known to affect confidentiality, integrity, and availability.

The advisory is shared for download at [gist.github.com](#). This vulnerability was named [CVE-2026-1879](#). The exploitation appears to be easy. The attack can be initiated remotely. Technical details and also a public exploit are known. The MITRE ATT&CK project declares the attack technique as [T1608.002](#).

It is possible to download the exploit at [gist.github.com](#). It is declared as proof-of-concept. The vendor was contacted early, responded in a very professional manner and quickly released a fixed version of the affected product.

Upgrading to version 6.10 eliminates this vulnerability. The upgrade is hosted for download at [github.com](#).

Product

Vendor

- [Harvard University](#)

Name

- [IQSS Dataverse](#)

Version

- [6.0](#)
- [6.1](#)
- [6.2](#)
- [6.3](#)
- [6.4](#)
- [6.5](#)
- [6.6](#)
- [6.7](#)
- [6.8](#)

CPE 2.3

- [🔒](#)
- [🔒](#)
- [🔒](#)

CPE 2.2

- [🔒](#)
- [🔒](#)
- [🔒](#)

CVSSv4

VuIDB Vector: [🔒](#)

VuIDB Reliability: [🔍](#)

CVSSv3

VuIDB Meta Base Score: 6.3

VuIDB Meta Temp Score: 5.7

VuIDB Base Score: 6.3

VuIDB Temp Score: 5.7

VuIDB Vector: [🔒](#)

VuIDB Reliability: [🔍](#)

CVSSv2

VulDB Base Score: 🔒

VulDB Temp Score: 🔒

VulDB Reliability: 🔍

Exploiting

Class: Unrestricted upload

CWE: [CWE-434](#) / [CWE-284](#) / [CWE-266](#)

CAPEC: 🔒

ATT&CK: 🔒

Physical: No

Local: No

Remote: Yes

Availability: 🔒

Access: Public

Status: Proof-of-Concept

Download: 🔒

Price Prediction: 🔍

Current Price Estimation: 🔒

Threat Intelligence

Interest: 🔍

Active Actors: 🔍

Active APT Groups: 🔍

Countermeasures

Recommended: Upgrade

Status: 🔍

0-Day Time: 🗝️

Upgrade: IQSS Dataverse 6.10

Timeline

- 04/01/2026 | Advisory disclosed
- 04/01/2026 | +0 days | VulDB entry created
- 04/01/2026 | +0 days | VulDB entry last update

Sources

Advisory: gist.github.com

Status: Confirmed

CVE: CVE-2026-1879 (🗝️)

GCVE (CVE): GCVE-0-2026-1879

GCVE (VulDB): GCVE-100-354616

scip Labs: <https://www.scip.ch/en/?labs.20161013>

Entry

Created: 04/01/2026 11:22 AM

Changes: 04/01/2026 11:22 AM (60)

Complete: 🔍

Submitter: JustF0rFun

Cache ID: 52:4EE:179

Submit

Accepted

- [Submit #749003](#): Harvard University Dataverse Project 6.8 build 1994-92d1ec8 Unrestricted Upload (by JustF0rFun)

Discussion

No comments yet. Languages: en.

Please log in to comment.