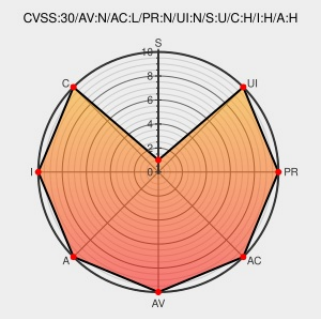
CVE-2015-9287

Published on: 05/13/2019 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:21 PM UTC

CVE-2015-9287

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of The University Of Cambridge Web Authentication System Apache Authentication Agent from Cam contain the following vulnerability:

Directory Traversal was discovered in University of Cambridge mod_ucam_webauth before 2.0.2. The key identification field ("kid") of the IdP's HTTP response message ("WLS-Response") can be manipulated by an attacker. The "kid" field is not signed like the rest of the message, and manipulation is therefore trivial. The "kid" field should only ever represent an integer. However, it is possible to provide any string value. An attacker could use this to their advantage to force the application agent to load the RSA public key required for message integrity checking from an unintended location.

CVE-2015-9287 has been assigned by cve@mitre.org to track the vulnerability - currently rated as CRITICAL severity.

CVSS3 Score: 9.8 - CRITICAL

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: 5 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	NONE	NONE

CVE References

Description	Tags	Link
GitHub - grymer/CVE	Third Party Advisory github.com text/html	MISC github.com/grymer/CVE
Raven Authentication Service | SpringerLink	Permissions Required Third Party Advisory doi.org text/html	MISC doi.org/10.1007/978-3-030-03251-7_1

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Cam	The University Of Cambridge Web Authentication System Apache Authentication Agent	All	All	All	All
Application	Cam	The University Of Cambridge Web Authentication System Apache Authentication Agent	All	All	All	All

cpe:2.3:a:cam:the_university_of_cambridge_web_authentication_system_apache_authentication_agent:*:*:*:*:*:*:*:*:

cpe:2.3:a:cam:the_university_of_cambridge_web_authentication_system_apache_authentication_agent:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→