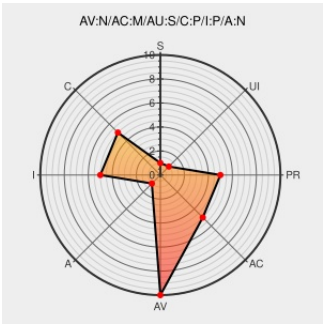
CVE-2012-3426

Published on: 07/31/2012 12:00:00 AM UTC

Last Modified on: 02/13/2023 04:13:23 AM UTC

CVE-2012-3426

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



Certain versions of Essex from Openstack contain the following vulnerability:

OpenStack Keystone before 2012.1.1, as used in OpenStack Folsom before Folsom-1 and OpenStack Essex, does not properly implement token expiration, which allows remote authenticated users to bypass intended authorization restrictions by (1) creating new tokens through token chaining, (2) leveraging possession of a token for a disabled user account, or (3) leveraging possession of a token for an account with a changed password.

CVE-2012-3426 has been assigned by secalert@redhat.com to track the vulnerability

CVSS2 Score: 4.9 - MEDIUM

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

CVE References

Description	Tags	Link
Security Advisory SA50045 - OpenStack Keystone Token Expiration Security Bypass Vulnerabilities - Secunia	web.archive.org text/html	SECUNIA 50045
Bug #996595 “[OSSA 2012-010] Following a password compromise and...” : Bugs : Keystone	bugs.launchpad.net text/html	CONFIRM bugs.launchpad.net/keystone/+bug/996595
oss-security - [OSSA 2012-010] Various Keystone token	Patch www.openwall.com	MLIST [oss-security] 20120727 [OSSA 2012-010] Various Keystone token expiratio issues (CVE-2012-3426)

expiration issues (CVE-2012-3426)	text/html	
USN-1552-1: OpenStack Keystone vulnerabilities | Ubuntu	www.ubuntu.com text/html	UBUNTU USN-1552-1
Bug #998185 “[OSSA 2012-010] Once a token is created/distributed...” : Bugs : OpenStack Identity (keystone)	bugs.launchpad.net text/html	CONFIRM bugs.launchpad.net/keystone/+bug/998185
Invalidate user tokens when a user is disabled · openstack/keystone@d960043 · GitHub	github.com text/html	CONFIRM github.com/openstack/keystone/commit/d9600434da14976463a0bd03abd8e0309f0db4
Carrying over token expiry time when token chaining · openstack/keystone@29e74e7 · GitHub	github.com text/html	CONFIRM github.com/openstack/keystone/commit/29e74e73a6e51cffc0371b32354558391826a4
Invalidate user tokens when password is changed · openstack/keystone@a67b248 · GitHub	github.com text/html	CONFIRM github.com/openstack/keystone/commit/a67b24878a6156eab17b9098fa649f0279256f5
Invalidate user tokens when a user is disabled · openstack/keystone@628149b · GitHub	Exploit Patch github.com text/html	CONFIRM github.com/openstack/keystone/commit/628149b3dc6b58b91fd08e6ca8d91c728ccb86
	Patch launchpad.net application/gzip	CONFIRM launchpad.net/keystone/essex/2012.1.1/+download/keystone-2012.1.1.tar.gz
Carrying over token expiry time when token chaining · openstack/keystone@375838c · GitHub	Patch github.com text/html	CONFIRM github.com/openstack/keystone/commit/375838cfceb88cacc312ff6564e64eb18ee6a35
Invalidate user tokens when password is changed · openstack/keystone@ea03d05 · GitHub	Exploit Patch github.com text/html	CONFIRM github.com/openstack/keystone/commit/ea03d05ed5de0c015042876100d37a6a14bf56
Bug #997194 “[OSSA 2012-010] Tokens remain valid after a user ac...” : Bugs : Keystone	bugs.launchpad.net text/html	CONFIRM bugs.launchpad.net/keystone/+bug/997194
Security Advisory SA50494 - Ubuntu update for keystone - Secunia	web.archive.org text/html	SECUNIA 50494

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Openstack	Essex	All	All	All	All
Application	Openstack	Essex	All	All	All	All
Application	Openstack	Horizon	folsom-1	All	All	All
Application	Openstack	Horizon	folsom-1	All	All	All
Application	Openstack	Keystone	2012.1	All	All	All
Application	Openstack	Keystone	2012.1.1	All	All	All
Application	Openstack	Keystone	2012.1	All	All	All
Application	Openstack	Keystone	2012.1.1	All	All	All

cpe:2.3:a:openstack:essex:*:*:*:*:*:*:*:*:

cpe:2.3:a:openstack:essex:*:*:*:*:*:*:*:*:

cpe:2.3:a:openstack:horizon:folsom-1:*:*:*:*:*:*:*:

cpe:2.3:a:openstack:horizon:folsom-1:*:*:*:*:*:*:*:

cpe:2.3:a:openstack:keystone:2012.1:*:*:*:*:*:*:*:

cpe:2.3:a:openstack:keystone:2012.1.1:*:*:*:*:*:*:*:

cpe:2.3:a:openstack:keystone:2012.1:*:*:*:*:*:*:*:

cpe:2.3:a:openstack:keystone:2012.1.1:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→