



Products

Services

Publications

Resources

What's new

Follow @Openwall on Twitter for new release announcements and other news

[<prev] [next>] [day] [month] [year] [list]

Message-ID: <50B63C17.2060806@openstack.org>
 Date: Wed, 28 Nov 2012 17:30:15 +0100
 From: Thierry Carrez <thierry@...nstack.org>
 To: "openstack@...ts.launchpad.net" <openstack@...ts.launchpad.net>,
 oss-security@...ts.openwall.com, openstack-announce@...ts.openstack.org
 Subject: [OSSA 2012-019] Extension of token validity through token chaining
 (CVE-2012-5563)

-----BEGIN PGP SIGNED MESSAGE-----
 Hash: SHA256

OpenStack Security Advisory: 2012-019
 CVE: CVE-2012-5563
 Date: November 28, 2012
 Title: Extension of token validity through token chaining
 Reporter: Anddy
 Products: Keystone
 Affects: Folsom, Grizzly

Description:

Anddy reported avulnerability in token chaining in Keystone. A token expiration date can be circumvented by creating a new token before the old one has expired. An authenticated and authorized user could potentially leverage this vulnerability to extend his access beyond the account owner expectations. Note: this vulnerability was fixed in the past (CVE-2012-3426) but was reintroduced in Folsom when code was refactored to support PKI tokens.

Grizzly (development branch) fix:
<https://github.com/openstack/keystone/commit/38c7e46a640a94da4da89a39a5a1ea9c081f1eb5>

Folsom fix (included in upcoming Keystone 2012.2.1 stable update):
<https://github.com/openstack/keystone/commit/f9d4766249a72d8f88d75dcf1575b28dd3496681>

References:
<https://bugs.launchpad.net/keystone/+bug/1079216>
<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=2012-5563>

- - -
 Thierry Carrez (ttx)
 OpenStack Vulnerability Management Team
 -----BEGIN PGP SIGNATURE-----
 Version: GnuPG v1.4.11 (GNU/Linux)
 Comment: Using GnuPG with undefined - <http://www.enigmail.net/>

iQIcBAEBCAAGBQJQtjwXAAoJEFB6+JAIsQJj3cwP/3FUjqWBxAHgRTMwz2Df5JML
 DZielkcq3kxSn05GCJ25FU5JyA3lWvqqoEsU4+SxytBTNAGYhDe8toSo74xU4PLU
 g3+A2V5oUMEJnyCS6ps7YMiLmd1unN3Fz/yrqxAZE7GRv+voD1l64+2IHK15bN7G
 WG+FxN3CgRK+pk+3MpPkaNLI1L9wTeYTPUgBdem+I7xhmLRsf5TB01gqu3gHja1+
 gvpWjezroWrVdAuqWFFsgzWf7LUZqZR/AqaWwS4DrHJ4LoD+ruHXNGvGyg1BQg8d
 IhqgAhBSdndlaJWTr6fj2KoqhpJK8Wu4VKIr9yIekbQIzJx11IYA9vjJ38eJ2v1
 x2NLnNDKrq2Q51l+iAy5MMbqmFwqljwZhpNFdW+ysybFMG1CtEnCgQPLqmbF9m9m
 8M9uV/vfGKuD73GpmMR7MLHldySv+uiqJnFzyCce+QMzP7enCBitBDp0t52dRal7
 TrTR7HGXIkJVJ4I/73o3MBAFQzrmTsSIYmuVybArnaNzvrct6aZTKH8hSPWRKVqx/
 pcBP7z+wLzHkJELWD0X9vgZJZJUj5qbMx6jq0NYYWY1lCrLTIRxXppS76/ZUzzIm
 qGS7FqUQM8u+x8rynnKNattFjW0dwXcFhcy3Io3Noc3kBDTgZf4fshBHWb00X0qf
 BI3upFpAwQ4g4ep16o1k
 =CZnJ
 -----END PGP SIGNATURE-----

Powered by blists - [more mailing lists](#)

Please check out the [Open Source Software Security Wiki](#), which is counterpart to this [mailing list](#).

Confused about [mailing lists](#) and their use? [Read about mailing lists on Wikipedia](#) and check out these [guidelines on proper formatting of your messages](#).