Alpine Linux - Bug #5288

Bug # 5285 (Closed): openssh: missing sanitisation of input for X11 forwarding (CVE-2016-3115)

[3.0] openssh: missing sanitisation of input for X11 forwarding (CVE-2016-3115)

03/18/2016 02:17 PM - Alicha CH

Status:	Closed	**Start date:**	03/18/2016
Priority:	Normal	**Due date:**	
Assignee:	Natanael Copa	**% Done:**	100%
Category:	Security	**Estimated time:**	0.00 hour
Target version:	3.0.7		
Affected versions:		**Security IDs:**	

Description

Missing sanitisation of untrusted input allows an authenticated user who is able to request X11 forwarding to inject commands to xauth(1).

Injection of xauth commands grants the ability to read arbitrary files under the authenticated user's privilege. Other xauth commands allow
limited information leakage, file overwrite, port probing and generally expose xauth(1), which was not written with a hostile user in mind, as an attack surface.

xauth(1) is run under the user's privilege, so this vulnerability offers no additional access to unrestricted accounts, but could circumvent key or account restrictions
such as sshd_config ForceCommand, authorized_keys command="..." or restricted shells.

Affected versions:

All versions of OpenSSH prior to 7.2p2 with X11Forwarding enabled.

Fixed In Version:

openssh 7.2p2

References:

http://www.openssh.com/txt/x11fwd.adv
https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2016-3115

Associated revisions

Revision b1a290f6 - 03/22/2016 11:56 AM - Leonardo Arena

main/openssh: security fix (CVE-2016-3115). Fixes #5288

History

#1 - 03/22/2016 11:57 AM - Leonardo Arena

- Status changed from New to Resolved

#2 - 03/23/2016 08:34 AM - Anonymous

- % Done changed from 0 to 100

Applied in changeset alpine:b1a290f67ac9baac539075e7c3bd5aa22e8d971a.

#3 - 03/23/2016 10:48 AM - Alicha CH

- Category set to Security

- Status changed from Resolved to Closed