pfSense - Bug #8153

Post-auth RCE in cert_get_publickey() from certs.inc, used in system_camanager.php and system_certmanager.php

12/01/2017 11:29 AM - Jim Pingle

Status:	Resolved	**Start date:**	12/01/2017
Priority:	Urgent	**Due date:**	
Assignee:	Jim Pingle	**% Done:**	100%
Category:	Certificates	**Estimated time:**	0.00 hour
Target version:	2.4.2-p1		
Plus Target Version:		**Affected Version:**	All
Release Notes:	Default	**Affected Architecture:**	

Description

cert_get_publickey() in source:src/etc/inc/certs.inc takes user input and uses it in a shell command without encoding, allowing a user to pass malicious input through system_camanager.php and system_certmanager.php during the import process via the cert and key fields.

This requires that the user be logged in and have access to system_camanager.php or system_certmanager.php

Affects 2.3.x in cert_get_modulus() which uses a similar operation, but only happens in system_certmanager.php when editing an existing CSR.

Associated revisions

Revision b6dcbd64 - 12/01/2017 11:41 AM - Jim Pingle

When retrieving a public key for a certificate, private key, or signing request, write the certificate data out to a temp file instead of echoing it through a pipe. Fixes #8153

Revision 552d7750 - 12/01/2017 11:43 AM - Jim Pingle

When retrieving a public key for a certificate, private key, or signing request, write the certificate data out to a temp file instead of echoing it through a pipe. Fixes #8153

(cherry picked from commit b6dcbd646feb9c7197b4e94a6031b69c2113d679)

Revision 6e316e95 - 12/01/2017 11:44 AM - Jim Pingle

When retrieving a the modulus for a certificate, private key, or signing request, write the certificate data out to a temp file instead of echoing it through a pipe. Fixes #8153

Revision d3e0194e - 12/01/2017 11:44 AM - Jim Pingle

When retrieving a the modulus for a certificate, private key, or signing request, write the certificate data out to a temp file instead of echoing it through a pipe. Fixes #8153

(cherry picked from commit 6e316e955350ad69d4f86cb332a1a48bfa028e2e)

History

#1 - 12/01/2017 11:35 AM - Jim Pingle

- Description updated

- Target version changed from 2.4.3 to 2.4.2-p1

#2 - 12/01/2017 12:00 PM - Jim Pingle

- Status changed from Confirmed to Feedback

- % Done changed from 0 to 100

Applied in changeset b6dcbd646feb9c7197b4e94a6031b69c2113d679.

#3 - 12/04/2017 09:46 AM - Jim Pingle

- Status changed from Feedback to Resolved

Fixed in current snapshots.

#4 - 12/14/2017 11:09 AM - Jim Pingle

- Private changed from Yes to No