Plesk

Plesk Sicherheitlücke (SQL Injection)

SYMPTOMS

SQL injection vulnerability within Plesk for Linux/Unix.

RESOLUTION

Please download the following file:

For Plesk v8.0.0 and v8.0.1 :
http://download1.swsoft.com/Plesk/Hotfix/PleskUnix/8.0.1/114298/class.Session.php
MD5 (class.Session.php) = 4d917ed483cbf030fb122a1e214b2bbf

For Plesk v8.1.0 :
http://download1.swsoft.com/Plesk/Hotfix/PleskUnix/8.1.0/114298/class.Session.php
MD5 (class.Session.php) = 4de3b2fc50011d27fb13e5a293720100

For Plesk 8.2.0 :
http://download1.swsoft.com/Plesk/Hotfix/PleskUnix/8.2.0/114298/class.Session.php
MD5 (class.Session.php) = 5b7a8071374aa94b83697aec72d1d556

and replace **/usr/local/psa/admin/plib/class.Session.php** file on Plesk server with the downloaded new one. Make sure that md5sum is correct after file is replaced, for example:

wget
http://download1.swsoft.com/Plesk/Hotfix/PleskUnix/8.2.0/114298/class.Session.php

md5sum ./class.Session.php
MD5 (./class.Session.php) = 5b7a8071374aa94b83697aec72d1d556

cp /usr/local/psa/admin/plib/class.Session.php
/usr/local/psa/admin/plib/class.Session.php.old

cp ./class.Session.php /usr/local/psa/admin/plib/class.Session.php

chgrp psaadm /usr/local/psa/admin/plib/class.Session.php

/usr/local/psa/admin/bin/httpsdctl restart

Plesk versions 7.5.4 and 8.1.1 are not affected by this vulnerability.

Quelle: http://kb.swsoft.com/en/2169

Eindeutige ID: #1049
Verfasser: Michael Stender
Letzte Änderung: 2007-09-22 17:59