Plesk

Plesk SQL Injektion

Am 10.02.12 erhielten wir folgende E-Mail von Parallels:

Dear Parallels Plesk Panel User:

Please read this message in its entirety and take the recommended actions.

Parallels has been informed of a SQL injection security vulnerability in some older versions of Plesk. This vulnerability is considered critical in nature and customers are advised take action quickly.

A **patch has been released** to resolve this vulnerability. Based on the version and operating system of Plesk you use, please **follow the instructions below.**

Linux

Plesk 10 - Update to Plesk 10.3.1 MicroUpdate #6 or later.
Update Instructions: here
If possible, it is recommended to update all the way to Plesk 10.4.4 to provide the most stable user experience.

Plesk 9 - Update to Plesk 9.5.4 MicroUpdate #11 or later
Update Instructions: here

Plesk 8 - Update to Plesk 8.6.0 MicroUpdate #2 or later
Update Instructions: here

Windows

Plesk 10 - Update to Plesk 10.3.1 MicroUpdate #6 or later.
Update Instructions: here
If possible, it is recommended to update all the way to Plesk 10.4.4 to provide the most stable user experience.

Plesk 9 - Apply Fix from Parallels Knowledge Base
Update Instructions: here

Plesk 8 - Apply Fix from Parallels Knowledge Base
Update Instructions: here

If you are already at or **above** the Version and MicroUpdate levels indicated above - you are **already protected** from this vulnerability.

Parallels takes the security of our customers very seriously and urges you to act quickly by applying these patches.

Thanks,

- The Parallels Plesk Panel Team

Leider wussten wir zu diesem Zeitpunkt noch nicht, das einer unserer Server bereits kompromitiert war.

Wer dieses Update noch nicht eingespielt hat, sollte dies umgehend nachholen. Leider heisst dies dann nicht, das der Server nicht bereits gehackt wurde. Jeder Admin sollte unbedingt die Logdateien genau durchsuchen, ob nicht bereits sämtliche Passwörter ausgelesen wurden.

Dies kann man wie folgt überprüfen:

Plesk

Zuerst schaut man sich unter /usr/local/psa/admin/logs die httpsd_access_log an. Nicht nur die sondern auch die gepackten logs, da der Angriff schon vor Wochen stattgefunden haben kann.

Sucht nach dem Eintrag:

"POST /enterprise/control/agent.php HTTP/1.1" 200 185 "-" "-"

Wenn ihr so etwas findet ist noch alles OK. Findet ihr aber so etwas:

"POST /enterprise/control/agent.php HTTP/1.1" 200 3775 "-" "-"

könnt ihr davon ausgehen, das der Angreifer alle eure Plesk Passwörter hat. Ist die Rot eingefärbte Zahl kleiner als 200 kb

Eindeutige ID: #1073
Verfasser: Michael Stender
Letzte Änderung: 2012-02-29 21:01