Sehr geehrte Kundinnen und Kunden,

ein kürzlich bekannt gewordener Fehler im Kernel erlaubt es Angreifern in einem Linux-System Dateien zu verändern, auf die sie keinen Zugriff haben dürften. So könnten sie sich Root-Rechte verschaffen und weitere Änderungen am System vornehmen. Die dafür veröffentlichte und als hoch eingestufte Schwachstelle „Dirty Pipe“ (CVE-2022-0847) wurde in den Kernelversionen 5.16.11, 5.15.25 und 5.10.102 geschlossen.

Wir sind bereits in direktem Austausch mit unseren Herstellern und prüfen, ob die Schwachstelle in deren Software eine Auswirkung hat. Bisher sind uns keine Probleme dazu bekannt.

Technische Details:
Pipes ermöglichen die unidirektionale Kommunikation zwischen Prozessen welche auf Unix-Systemen zum Einsatz kommen. Das Besondere dabei ist, dass keine Daten im Speicher kopiert werden müssen, was Zeit kosten würde. Problematisch wird es, wenn mehrere Absender eine Pipe mit Daten beschicken. Das Verwalten dieser Verweise und Speicherbereiche und der damit verbundenen Rechte ist Aufgabe des Kernels. Die „Dirty Pipe“ Schwachstelle ermöglicht es, dies zu umgehen.

Betroffene Versionen:
Das Problem betrifft alle Systeme, die Linux ***ab Kernel Version 5.8*** einsetzen. Dies sind neben Client- und Server Systemen ggfs. auch Embedded Systeme in IoT Devices und Mobilgeräte wie Smartphones und Tablets

Infoquellen/Referenzen:
https://www.heise.de/news/Linux-Dirty-Pipe-beschert-Root-Rechte-6541556.html
https://dirtypipe.cm4all.com/

Unsere empfohlenen Maßnahmen dazu:
Prüfen Sie die Verfügbarkeit von Updates zu dieser Schwachstelle in Ihrer Linux Umgebung. Diese sollten dann möglichst zeitnah aktualisiert werden. Sobald wir weitere Informationen und Details erhalten, werden wir die entsprechenden Informationen in Form eines Updates dieses Artikels bereitstellen.

Bei Fragen zu diesem Thema unterstützen wir Sie gerne unter **support@bacher.at** oder +43 60 126-34. Falls die erforderliche Maßnahme nicht durch Ihren Betriebsführungs- oder Support-Vertrag abgedeckt ist, bieten wir Ihnen auf Rückfrage gerne an, die Arbeiten durch unsere Spezialisten durchzuführen.

Mit freundlichen Grüßen
Bacher Systems Support Team

Dear valued customer,

a recently discovered issue within the kernel allows attackers to change files on a Linux system they shouldn't have access to. This could be used for privilege escalation or to perform further unwanted changes. The so called „dirty pipe" vulnerability, rated with severity high, was released as CVE-2022-0847 and solved in kernel versions 5.16.11, 5.15.25 and 5.10.102.

We are in direct contact with our vendors to check possible effects to their software. Currently we do not have any information on related issues here.

Technical details:
Pipes allow one-way communication between processes in Unix environments. Their advantage is that no data needs to be copied into memory, which would cause delay. In case several senders address a pipe with data, this can lead to problems. The kernel is responsible managing those links and memory areas and related privileges. The "Dirty pipe" vulnerability allows to bypass this protection mechanism.

Affected versions:
All Linux kernel **versions from 5.8 and above**. Besides client and server systems, possibly also embedded systems in IOT devices or mobile phones and tablets.

Sources/references:
https://www.heise.de/news/Linux-Dirty-Pipe-beschert-Root-Rechte-6541556.html
https://dirtypipe.cm4all.com/

Our recommendations:
Please check available updates for your specific Linux environment and install them as soon as possible. Any updates on our part will be communicated by additional information in this newsletter.

If you have any further questions, please do not hesitate to contact us at **support@bacher.at** or +43 1 60 126-34. In case this is not already covered by your operational contract we gladly offer on request to have this change implemented by one of our engineers.

Best regards
Bacher Systems Support Team