Sehr geehrte Kundinnen und Kunden,

mit diesem Newsletter möchten wir Sie über ein mögliches Problem in der **Check Point Identity Awareness Funktion** informieren. Check Point bietet **zwei Möglichkeiten** (AD-Query oder Identity Collector) um Benutzer- und Computerinformationen aus dem Active Directory auszulesen.

Demnächst werden in Microsofts DCOM Prozess Verbesserungen zur Sicherheit (CVE-2021-26414) eingeführt. Es wird dadurch ein höheres Authentifizierungslevel erforderlich, um über DCOM Abfragen durchführen zu können. Danach ist diese Schnittstelle nicht mehr in gewohnter Weise nutzbar und das kann zu Problemen führen.

Check Point AD Query und Identity Logging erhält User- und Computerinformationen aus den Microsoft Security Event Logs. Die Abfrage erfolgt über das WMI Service von Microsoft, welches wiederum den DCOM Prozess verwendet.
Wenn Sie noch AD-Query zur Identity Abfrage nutzen, sind Sie von dieser bevorstehenden Umstellung ab **14. Juni 2022**. betroffen. Bitte beachten Sie den dahinterliegenden Zeitplan von Microsoft:

- **8. Juni 2021**: Microsoft hat die Änderungen über ein Softwareupdate ermöglicht, aber nicht automatisch aktiviert. Über Anpassung der Windows Registry können diese aktiviert werden.
- **14. Juni 2022**: Microsoft aktiviert die Absicherung des DCOM Prozesses, mit der Möglichkeit es über die Windows Registry zu deaktivieren.
- **14. März 2023**: Microsoft aktiviert die Absicherung des DCOM Prozesses. Es gibt keine Möglichkeit diese Änderung zu umgehen.

Nach Aktivierung dieser Verbesserungen, können Identity Awareness Abfragen nicht mehr in gewohnter Weise das WMI Service erfolgen. Die Abfragen werden geblockt, Benutzer- und Computerinformation sind nicht mehr nutzbar.

Betroffene Versionen:

- Check Point Gateways, die AD Query als Identity Awareness Quelle nutzen
- Check Point Management Umgebungen, die Identity Logging aktiviert haben

Infoquellen/Referenzen:
Microsoft KB5004442
Check Point SK176148

Unsere empfohlenen Maßnahmen dazu:
Bitte überprüfen Sie Ihre Konfiguration und treffen Sie zeitgerecht Maßnahmen, um Probleme zu vermeiden. Check Point und Bacher Systems empfehlen den **Umstieg auf den Check Point Identity Collector** als Quelle für Benutzer und Computerinformationen. Dieser ist nicht von der Änderung im DCOM Prozess betroffen und bietet weitere wesentliche Vorteile gegenüber AD Query.
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
Ihr Bacher Support Team

Dear Customer,

with this newsletter we would like to inform you about a potential problem in **Check Point's Identity Awareness function**. Check Point offers **two options** (AD Query or Identity Collector) to read user and computer information from the Active Directory.

Microsoft will soon introduce security related enhancements on its DCOM process due to a known vulnerability (CVE-2021-26414). As a result, a higher level of authentication is required in order to carry out queries via DCOM . After that, this interface can no longer be used the usual way which can lead to problems.
Check Point AD Query and Identity Logging obtain user and computer information from Microsoft Security Event Logs. The query is made via Microsoft's WMI service, which in turn uses the DCOM process. If you're still using AD-query for identity requests you're affected by **June 14th 2022**. Please examine the details and Microsofts' schedule for that:

- **June 8th, 2021**: Hardening changes disabled by default but with the ability to enable them using a registry key.
- **June 14th, 2022:** Hardening changes enabled by default but with the ability to disable them using a registry key.
- **March 14th, 2023**: Hardening changes enabled by default with no ability to disable them. By this point, you must resolve any compatibility issues with the hardening changes and applications in your environment.

After activating these improvements were, Identity Awareness queries can no longer be carried out in the usual way using the WMI service. The queries will be blocked, user and computer information can no longer be used.

Affected versions:

- Check Point gateways, using AD-query as Identity Awareness source
- Check Point management with activated identity logging

Sources/references:
Microsoft KB5004442
Check Point SK176148

Our Recommendations:
Please check your configuration and take timely action to avoid problems. Check Point and Bacher Systems recommend switching to **Check Point Identity Collector** as the source for user and computer information. This type of implementation is not affected by the change in the DCOM process and offers other significant advantages over AD-query.
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