Sehr geehrte Kundinnen und Kunden,

wir informieren Sie über eine kürzlich bekannt gewordene Schwachstelle (CVE-2022-0778) mit Schweregrad hoch, in der weit verbreiteten Software für Transportverschlüsselung auf Basis OpenSSL. Bei der Verarbeitung von bestimmten TLS-Zertifikaten kann es dadurch zu Fehlern kommen. Ein anonymer Angreifer kann diese Schwachstelle remote ausnutzen, um einen Denial of Service Angriff durchzuführen.

Einige Hersteller aus unserem Portfolio sind betroffen und bieten bereits Updates an, um diese Schwachstelle zu schließen oder zu reduzieren. Wir beobachten die Situation bereits seit mehreren Tagen, die Angaben zu den Updates sind derzeit noch nicht vollständig überschaubar. Eventuell werden in den nächsten Tagen weitere Produkte als verwundbar identifiziert.

Es folgt eine Übersicht der Hersteller, und der jeweilige Status, soweit uns dieser derzeit bekannt ist. Bitte prüfen Sie in den nächsten Tagen aktiv auf unserer Webseite, ob wir weitere Hersteller ergänzen oder die Hersteller unter den angeführten Links zusätzliche Updates veröffentlichen.

Hersteller	Status	Version	Link zur Knowledge Base
Check Point	betroffen	Alle	Siehe KB
Cyber Ark	in Prüfung		
Trend Micro	in Prüfung		
RSA	in Prüfung		
Radware	in Prüfung		
VMWare	in Prüfung		
Thales	in Prüfung		
Netapp	betroffen	Siehe KB	Siehe KB
Tenable	betroffen		Siehe KB
Nutanix	in Prüfung		
Commvault	nicht betroffen		
Veritas Netbackup	nicht betroffen		
Splunk	in Prüfung		

Infoquellen/Referenzen:
Heise.de
CVE.org

Unsere empfohlenen Maßnahmen dazu:
Folgen Sie den Hinweisen der Hersteller und führen Sie die entsprechenden Update Schritte durch. Derzeit sind uns keine weiteren Details anderer Hersteller und Lösungen bekannt. Wir werden diese gegebenenfalls in einem Update nachliefern.

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 recently released vulnerability (CVE-2022-0778) rated with severity high. The broadly used software for transport encryption, based on OpenSSL, is affected. The vulnerability may cause abnormal behavior when parsing an invalid certificate. This can be exploited remotely and could be subject to a denial of service attack.

Several of our vendors already delivered updates to patch this vulnerability or to mitigate it. We are monitoring the situation for several days now. Be aware that the full impact and available updates are not completely explored and may change within the next days. Additional updates may come over the next days.
Here is a list of vendors and their status on vulnerability and software updates. Please monitor the Bacher newsroom actively for possible changes over the next days.

Vendor	Status	Version	Link to knowledge base
Check Point	yes	all	Siehe KB
Cyber Ark	under investigation		
Trend Micro	under investigation		
RSA	under investigation		
Radware	under investigation		
VMWare	under investigation		
Thales	under investigation		
Netapp	yes	Siehe KB	Siehe KB
Tenable	yes		Siehe KB
Nutanix	under investigation		
Commvault	not vulnerable		
Veritas Netbackup	not vulnerable		
Splunk	under investigation		

Infoquellen/Referenzen:
Heise.de
CVE.org

Our recommendation:
Follow the given procedures for each solution and implement the updates. Any possible updates on our part will be communicated by additional information.

We are at your disposal in case you need assistance or if you have questions. You can 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