Sehr geehrte Kundinnen und Kunden,

Trend Micro hat auf unterschiedlichen Plattformen zu seinem Produkt Server Protect hoch eingestufte Schwachstellen erkannt. Dadurch sind Denial of Service Attacken oder ein Ausführen von schadhaftem Code möglich. Seit Kurzem stehen nun Updates zur Verfügung, die diese Schwachstellen beheben.

Betroffene Lösungen:
ServerProtect für Storage (SPFS) 6.0, Windows, Englisch
ServerProtect für Microsoft Windows / Novell NetWare (SPNT) 5.8, Windows, Englisch
ServerProtect für EMC Celerra (SPEMC) 5.8, EMC Celerra, Englisch
ServerProtect für Network Appliance Filers (SPNAF) 5.8, Network Appliance, Englisch

Infoquellen/Referenzen:
Trend Micro KB

Unsere empfohlenen Maßnahmen dazu:
Um die Schwachstelle ausnutzen zu können, ist ein Zugriff auf das betroffene System nötig. Installieren Sie die von Trend Micro bereit gestellten Updates schnellstmöglich. Ist eine zeitnahe Installation nicht möglich, prüfen Sie die Zugriffsmöglichkeiten auf betroffene Systeme und schränken diese gegebenenfalls ein.

Bei Fragen zu diesem Thema unterstützen wir Sie gerne unter **support@bacher.at** oder +43 1 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,

Trend Micro identified several high rated vulnerabilities for its product Server Protect on different platforms. An attacker could start denial of service attacks or execute malicious code. Updates were released recently to address those vulnerabilities.

Affected solutions:
ServerProtect for Storage (SPFS) 6.0, Windows, English
ServerProtect for Microsoft Windows / Novell NetWare (SPNT) 5.8, Windows, English
ServerProtect for EMC Celerra (SPEMC) 5.8, EMC Celerra, English
ServerProtect for Network Appliance Filers (SPNAF) 5.8, Network Appliance, English

Sources/references:
Trend Micro KB

Our Recommendations:
To exploit the vulnerabilities access to the affected system is necessary. Update the product with the new software provided by Trend Micro. In addition to timely application of patches and updated solutions, customers are also advised to review remote access to critical systems and restrict them if feasible.
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