Sehr geehrte Kundinnen und Kunden,

Cisco hat kürzlich eine mit Schweregrad hoch eingestufte Sicherheitslücke in der TACACS+ and RADIUS Authentifizierung seiner Cisco NX-OS Software veröffentlicht. Die Sicherheitslücke kann nur unter Verwendung von Telnet oder direkt auf dem Konsolenzugang des Geräts ausgenutzt werden. SSH Verbindungen sind nicht betroffen. Wenn diese Sicherheitslücke erfolgreich ausgenutzt wird, ermöglicht es Angreifern das Gerät neu zu starten und in einen Denial-of-Service Zustand zu versetzen.

Betroffene Devices:
MDS 9000 Series Multilayer Switches
Nexus 1000 Virtual Edge für VMware vSphere
Nexus 1000V Switch für Microsoft Hyper-V und VMware vSphere
Nexus 3000 Series Switches
Nexus 5500 und 5600 Platform Switches
Nexus 6000 und 7000 Series Switches
Nexus 9000 Series Switches im standalone NX-OS mode

Infoquellen/Referenzen:
Cisco Security Advisories

Unsere empfohlenen Maßnahmen dazu:
Installieren Sie dringend die von Cisco zur Verfügung gestellten Updates und Firmware Patches. Diese finden Sie unter dem oben angeführten Link. Sollten Sie die Updates/Patches nicht gleich einbringen können, kann der „directed request Support for TACACS+ or RADIUS“ als Workaround auf den betroffenen Devices deaktiviert werden, sofern dieses Service nicht unbedingt erforderlich ist.

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,

Cisco recently announced a new vulnerabilty in TACACS+ and RADIUS remote authentication for Cisco NX-OS with a severity high rating. This vulnerability can only be exploited over Telnet or over the console management connection. SSH connections to the device are not affected. A successful exploit could allow an attacker to cause the affected device to unexpectedly reload, resulting in a denial of service (DoS) condition.

Affected solutions:
MDS 9000 Series Multilayer Switches
Nexus 1000 Virtual Edge for VMware vSphere
Nexus 1000V Switch for Microsoft Hyper-V and VMware vSphere
Nexus 3000 Series Switches
Nexus 5500 and 5600 Platform Switches
Nexus 6000 and 7000 Series Switches
Nexus 9000 Series Switches in standalone NX-OS mode

Sources/references:
Cisco Security Advisories

Our Recommendations:
Immediately install the firmware patches Cisco provided on the given link. As a quick workaround directed request support for TACACS+ or RADIUS can be disabled if the service is not required on affected devices.
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