Sehr geehrte Kundinnen und Kunden,

Cisco hat kürzlich eine mit Schweregrad hoch eingestufte Sicherheitslücke im Cisco Discovery Protocol (CDP) veröffentlicht. Die Sicherheitslücke befindet sich auf den im nächsten Absatz angeführten Devices mit dem Betriebssystem NX-OS oder FXOS, wenn CDP aktiviert ist. Da dieses Protokoll am zweiten Layer des OSI-Schichten Modells operiert, muss sich der Angreifer in derselben Broadcast Domain wie das betroffene Device befinden.
Diese Sicherheitslücke ermöglicht es Angreifern auf dem Device Code mit privilegierten root-Rechten auszuführen. Darüber hinaus kann das Device rebootet und in einen Denial-of-Service Zustand versetzt werden.

**Betroffene Devices:**
Firepower 4100 Series
Firepower 9300 Security Appliances
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 Fabric Switches in ACI mode
Nexus 9000 Series Switches im standalone NX-OS mode
UCS 6200, 6300 und 6400 Series Fabric Interconnects

**Infoquellen/Referenzen:**
Weitere Details zur Sicherheitslücke und den betroffenen Cisco Devices finden Sie unter diesem Link
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cdp-dos-ce-wWvPucC9

**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 CDP als Workaround auf den betroffenen Devices deaktiviert werden.

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 Customers,

Cisco recently announced a new vulnerabilty in the Cisco Discovery Protocol (CDP) with a severity high rating. This vulnerability applies to the devices listed below running NX-OS or FXOS and having CDP enabled. Since this protocol operates on the 2nd OSI network layer the attacker needs to be within the same broadcast domain as the affected device.
This vulnerabilty allows attackers to execute arbitrary code with extended root-privileges. Furthermore it can generate reloads on the affected devices causing a denial of service condition.

**Affected devices:**
Firepower 4100 Series
Firepower 9300 Security Appliances
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 Fabric Switches in ACI mode
Nexus 9000 Series Switches in standalone NX-OS mode
UCS 6200, 6300 and 6400 Series Fabric Interconnects

**Sources/references:**
You can find details about this vulnerability and affected Cisco devices on this link
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-nxos-cdp-dos-ce-wWvPucC9

**Our Recommendations:**
Immediately install the firmware patches Cisco provided on the given link. As a quick workaround you can also disable the CDP on the 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