Betreff: [Ticketnummer] Offene Telnet-Server in AS[ASN]
***** Sicherheitsinformation / Security advisory *****
[English version below]
Sehr geehrte Damen und Herren,
Telnet ist ein veraltetes Netzwerkprotokoll für den textbasierten Fernzugriff auf Systeme. Die gesamte Kommunkation inklusive der Übermittlung von Benutzername und Passwort erfolgt bei Telnet unverschlüsselt im Klartext und kann somit potenziell von einem Angreifer auf dem Übertragungsweg mitgelesen werden.
Auf vielen IoT-Geräten (Router, IP-Kameras, etc.) ist standardmäßig ein Telnet-Server aktiv. Sind diese Geräte offen aus dem Internet erreichbar und wurden die Standard-Zugangsdaten nicht geändert, können Angreifer leicht die Kontrolle über diese Geräte erlangen. Schadsoftware wie Mirai nutzt dies aus, um automatisiert Geräte zu kompromittieren und einem Botnetz anzuschließen.
CERT-Bund empfiehlt für einen sicheren Fernzugriff auf Systeme die Nutzung von (Open)SSH mit schlüsselbasierter Authentisierung.
Im Anhang senden wir Ihnen eine Liste betroffener IP-Adressen in Ihrem Netzbereich. Der Zeitstempel (Zeitzone UTC) gibt an, wann unter der jeweiligen IP-Adresse ein offen aus dem Internet erreichbarer Telnet-Server identifiziert wurde.
Wir möchten Sie bitten, den Sachverhalt zu prüfen und Maßnahmen zur Absicherung der Systeme zu ergreifen bzw. Ihre Kunden entsprechend zu informieren.
Falls Sie kürzlich bereits Gegenmaßnahmen getroffen haben und diese Benachrichtigung erneut erhalten, beachten Sie bitten den angegebenen Zeitstempel. Wurde die Gegenmaßnahme erfolgreich umgesetzt, sollten Sie keine Benachrichtigung mit einem Zeitstempel nach der Umsetzung mehr erhalten.
Weitere Informationen zu dieser Benachrichtigung, Hinweise zur Behebung gemeldeter Sicherheitsprobleme sowie Antworten auf häufig gestellte Fragen finden Sie unter:
<https://reports.cert-bund.de/>
Diese E-Mail ist mittels PGP digital signiert.
Informationen zu dem verwendeten Schlüssel finden Sie unter:
<https://reports.cert-bund.de/digitale-signatur>
Bitte beachten Sie:
Dies ist eine automatisch generierte Nachricht. Antworten an die Absenderadresse <reports@reports.cert-bund.de> werden NICHT gelesen und automatisch verworfen. Bei Rückfragen wenden Sie sich bitte unter Beibehaltung der Ticketnummer [CB-Report#...] in der Betreffzeile an <certbund@bsi.bund.de>.
!! Bitte lesen Sie zunächst unsere HOWTOs und FAQ, welche unter
!! <https://reports.cert-bund.de/> verfügbar sind.
==========
Dear Sir or Madam,
Telnet is an outdated network protocol for text-oriented command-line access to remote hosts. With Telnet, all communication including username and password is transmitted unencrypted in clear text and is therefore susceptible to eavesdropping.
Many IoT devices (routers, network cameras, etc.) are running Telnet servers by default. If the devices are openly accessible from the Internet and standard login credentials have not been changed, an attacker can easily gain full control of the devices. Malware like Mirai automatically exploits insecure Telnet servers openly accessible from the Internet using to compromise devices and connect them to a botnet.
CERT-Bund recommends using (Open)SSH with key-based authentication for secure access to remote hosts.

Please find attached a list of affected IP addresses on your network.
The timestamp (timezone UTC) indicates when the openly accessible
Telnet server was identified.
We would like to ask you to check this issue and take appropriate
steps to secure affected systems or notify your customers accordingly.
If you have recently solved the issue but received this notification
again, please note the timestamp included below. You should not
receive any further notifications with timestamps after the issue
has been solved.
Additional information on this notification, advice on how to fix
reported issues and answers to frequently asked questions:
<https://reports.cert-bund.de/en/>
This message is digitally signed using PGP.
Information on the signature key is available at:
<https://reports.cert-bund.de/en/digital-signature>
Please note:
This is an automatically generated message. Replies to the
sender address <reports@reports.cert-bund.de> will NOT be read
but silently be discarded. In case of questions, please contact
<certbund@bsi.bund.de> and keep the ticket number [CB-Report#...]
of this message in the subject line.
!! Please make sure to consult our HOWTOs and FAQ available at
!! <https://reports.cert-bund.de/en/> first.
Mit freundlichen Grüßen / Kind regards
Team CERT-Bund
Bundesamt für Sicherheit in der Informationstechnik
Federal Office for Information Security (BSI)
Referat OC22 - CERT-Bund
Godesberger Allee 185-189, 53175 Bonn, Germany