Risks of Default Passwords on the Internet | CISA

Published: 2016-10-07 · Archived: 2026-04-06 01:10:42 UTC

Systems Affected

Any system using password authentication accessible from the internet may be affected. Critical infrastructure and other important embedded systems, appliances, and devices are of particular concern.

Overview

Attackers can easily identify and access internet-connected systems that use shared default passwords. It is imperative to change default manufacturer passwords and restrict network access to critical and important systems.

What Are Default Passwords?

Factory default software configurations for embedded systems, devices, and appliances often include simple, publicly documented passwords. These systems usually do not provide a full operating system interface for user management, and the default passwords are typically identical (shared) among all systems from a vendor or within product lines. Default passwords are intended for initial testing, installation, and configuration operations, and many vendors recommend changing the default password before deploying the system in a production environment.

What Is the Risk?

Attackers can easily obtain default passwords and identify internet-connected target systems. Passwords can be found in product documentation and compiled lists available on the internet. It is possible to identify exposed systems using search engines like Shodan, and it is feasible to scan the entire IPv4 internet, as demonstrated by such research as

- Shiny Old VxWorks Vulnerabilities
- Security Flaws in Universal Plug and Play: Unplug, Don't Play
- Serial Offenders: Widespread Flaws in Serial Port Servers
- The Wild West
- Internet Census 2012

Attempting to log in with blank, default, and common passwords is a widely used attack technique.

Impact

An attacker with knowledge of the password and network access to a system can log in, usually with root or administrative privileges. Further consequences depend on the type and use of the compromised system.

Examples of incident activity involving unchanged default passwords include

- Internet Census 2012 Carna Botnet distributed scanning
- Fake Emergency Alert System (EAS) warnings about zombies
- Stuxnet and Siemens SIMATIC WinCC software
- Kaiten malware and older versions of Microsoft SQL Server
- SSH access to jailbroken Apple iPhones
- Cisco router default Telnet and enable passwords
- SNMP community strings

Solution

Change Default Passwords

Change default passwords as soon as possible and absolutely before deploying the system on an untrusted network such as the internet. Use a sufficiently strong and unique password. See US-CERT Security Tip ST04-002 and *Password Security, Protection, and Management* for more information on password security.

Use Unique Default Passwords

Vendors can design systems that use unique default passwords. Such passwords may be based on some inherent characteristic of the system, like a MAC address, and the password may be physically printed on the system.

Use Alternative Authentication Mechanisms

When possible, use alternative authentication mechanisms like Kerberos, x.509 certificates, public keys, or multi-factor authentication. Embedded systems may not support these authentication mechanisms and the associated infrastructure.

Force Default Password Changes

Vendors can design systems to require password changes the first time a default password is used. Recent versions of DD-WRT wireless router firmware operate this way.

Restrict Network Access

Restrict network access to trusted hosts and networks. Only allow internet access to required network services, and unless absolutely necessary, do not deploy systems that can be directly accessed from the internet. If remote access is required, consider using VPN, SSH, or other secure access methods and be sure to change default passwords.

Vendors can design systems to only allow default or recovery password use on local interfaces, such as a serial console, or when the system is in maintenance mode and only accessible from a local network.

Identify Affected Products

It is important to identify software and systems that are likely to use default passwords. The following list includes software, systems, and services that commonly use default passwords:

- Routers, access points, switches, firewalls, and other network equipment
- Databases
- Web applications
- Industrial Control Systems (ICS) systems
- Other embedded systems and devices
- Remote terminal interfaces like Telnet and SSH
- Administrative web interfaces

Running a vulnerability scanner on your network can identify systems and services using default passwords. Freely available scanners include Metasploit and OpenVAS.

References

The Risk of Default Passwords

SHODAN - Computer Search Engine

Shiny Old VxWorks Vulnerabilities

Security Flaws in Universal Plug and Play: Unplug, Don't Play

Serial Offenders: Widespread Flaws in Serial Port Servers

The Wild West

Internet Census 2012

Zombie hack blamed on easy passwords

Secure EAS Codec s Prevent Zombie Attacks

SCADA System's Hard-Coded Password Circulated Online for Years

After Worm, Siemens Says Don't Change Passwords

"Kaiten" Malicious Code Installed by Exploiting Null Default Passwords in Microsoft SQL Server

Web Interface - DD-WRT Wiki

Penetration Testing Software | Metasploit

Open Vulnerability Assessment System

Revisions

Initial release

Source: https://www.us-cert.gov/ncas/alerts/TA13-175A