# CWE Detail – CWE-1277

## Description

The product does not provide its
 users with the ability to update or patch its
 firmware to address any vulnerabilities or
 weaknesses that may be present.

## Extended Description

Without the ability to
 patch or update firmware, consumers will be
 left vulnerable to exploitation of any known
 vulnerabilities, or any vulnerabilities that
 are discovered in the future. This can expose
 consumers to permanent risk throughout the
 entire lifetime of the device, which could be
 years or decades. Some external protective
 measures and mitigations might be employed to
 aid in preventing or reducing the risk of
 malicious attack, but the root weakness cannot
 be corrected.

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Observed Examples (CVEs)

**•** CVE-2020-9054: Chain: network-attached storage (NAS) device has a critical OS command injection (CWE-78) vulnerability that is actively exploited to place IoT devices into a botnet, but some products are "end-of-support" and cannot be patched (CWE-1277). [REF-1097] (KEV)

**•** [REF-1095]: A hardware "smart lock" has weak key generation that allows attackers to steal the key by BLE sniffing, but the device's firmware cannot be upgraded and hence remains vulnerable [REF-1095].

## Related Attack Patterns (CAPEC)

* CAPEC-682

## Modes of Introduction

**•** Requirements: Requirements development might not consider the importance of updates over the lifetime of the product, or might not choose the ability due to concerns such as expense or speed to market.

**•** Architecture and Design: Lack of planning during architecture development and design, or external pressures such as speed to market, could ignore the capability to update.

**•** Implementation: The weakness can appear through oversight during implementation.

## Common Consequences

**•** Impact: Gain Privileges or Assume Identity, Bypass Protection Mechanism, Execute Unauthorized Code or Commands, DoS: Crash, Exit, or Restart — Notes: If an attacker can identify an exploitable vulnerability in one device that has no means of patching, the attack may be used against an entire class of devices.

## Potential Mitigations

**•** Requirements: Specify requirements to include the ability to update the firmware. Include integrity checks and authentication to ensure that untrusted firmware cannot be installed. (Effectiveness: N/A)

**•** Architecture and Design: Design the device to allow for updating the firmware. Ensure that the design specifies how to distribute the updates and ensure their integrity and authentication. (Effectiveness: N/A)

**•** Implementation: Implement the necessary functionality to allow the firmware to be updated. (Effectiveness: N/A)

## Applicable Platforms

**•** None (Class: Not Language-Specific, Prevalence: Undetermined)

## Demonstrative Examples

**•** N/A

## Notes

**•** Terminology: The "firmware" term does not have a single commonly-shared definition, so there may be variations in how this CWE entry is interpreted during mapping.