# Internet of Things Top Ten





# Agenda

- Introduction
- Misconception
- Considerations
- The OWASP Internet of Things Top 10 Project
- The Top 10 Walkthrough





# 26 Billion by 2020

- 30 fold increase from 2009 in Internet of Things install base
- Revenue exceeding \$300 billion in 2020
- \$1.9 trillion in global economic impact

\*Gartner Internet of Things Report 2013





### Misconception | It's all about the device

- It's not just about the device, or the network, or the clients
- There are MANY surface areas involved
- Each of these need to be evaluated





### Considerations | A holistic approach is required

- All elements need to be considered
  - The Internet of Things Device
  - The Cloud
  - The Mobile Application
  - The Network Interfaces
  - The Software
  - Use of Encryption
  - Use of Authentication
  - Physical Security
  - USB ports
- Enter the OWASP Internet of Things Top Ten Project





### Internet of Things Top Ten Project | A complete IoT Review



- Review all aspects of Internet of Things
- Top Ten Categories
- Covers the entire device
- Without comprehensive coverage like this it would be like getting your physical but only checking one arm
- We must cover all surface area to get a good assessment of overall security





# I1 | Insecure Web Interface

Threat Agents	Attack Vectors	Security Weakness		Technical Impacts	<b>Business Impacts</b>
Application Specific	Exploitability EASY	Prevalence COMMON	Detectability EASY	Impact SEVERE	Application / Business Specific
Consider anyone who	Attacker uses weak	An insecure web interface	can be present when	Insecure web interfaces	Consider the business
has access to the web	credentials, captures	issues such as account er	numeration, lack of	can result in data loss or	impact of poorly secured
interface including	plain-text credentials or	account lockout or weak credenitals are present.		corruption, lack of	web interfaces that could
internal and external	enumerates accounts to	Insecure web interfaces a	Insecure web interfaces are prevalent as the intent		lead to compromised
users.	access the web interface.	is to have these interfaces	is to have these interfaces exposed only on internal		devices along with
	Attack could come from	networks, however threats	from the internal users	complete device	compromised customers.
	external or internal users.	can be just as significant a	as threats from external	takeover.	Could your customers be
		users. Issues with the web	interface are easy to		harmed? Could your
		discover when examining	the interface manually		brand be harmed?
		along with automated test	ing tools to identify other		
		issues such as cross-site	scripting.		





# I1 | Insecure Web Interface | Testing

#### Is My Web Interface Secure?

Checking for an Insecure Web Interface includes:

- Determining if the default username and password can be changed during initial product setup
- Determining if a specific user account is locked out after 3 5 failed login attempts
- Determining if valid accounts can be identified using password recovery mechanisms or new user pages
- Reviewing the interface for issues such as cross-site scripting, crosssite request forgery and sql injection.

- Account Enumeration
- Weak Default Credentials
- Credentials Exposed in Network Traffic
- Cross-site Scripting (XSS)
- SQL-Injection
- Session Management
- Account Lockout

#### **Example Attack Scenarios**

Scenario #1: The web interface presents "Forgot Password" functionality which upon entering an invalid account informs the attacker that the account does not exist. Once valid accounts are identified, password guessing can begin for an indefinite amount of time if no account lockout controls exist.

```
Account john@doe.com does not exist.
```

Scenario #2: Web interface is susceptible to cross-site scripting.

```
http://xyz.com/index.php?user=<script>alert(123) </script> ... Response from browser is an alert popup.
```

In the cases above, the attacker is able to easily determine if an account is valid or not and is also able to determine that the site is susceptible to cross-site scripting (XSS).





### I1 | Insecure Web Interface | Make It Secure

#### How Do I Make My Web Interface Secure?

A secure web interface requires:

- Default passwords and ideally default usernames to be changed during initial setup
- Ensuring password recovery mechanisms are robust and do not supply an attacker with information indicating a valid account
- 3. Ensuring web interface is not susceptible to XSS, SQLi or CSRF
- Ensuring credentials are not exposed in internal or external network traffic
- 5. Ensuring weak passwords are not allowed
- 6. Ensuring account lockout after 3 -5 failed login attempts

Please review the following tabs for more detail based on whether you are a Manufacturer &, Developer or Consumer &





### I2 | Insufficient Authentication/Authorization

Threat Agents	Attack Vectors	Security Weakness		Technical Impacts	Business Impacts
Application Specific	Exploitability AVERAGE	Prevalence COMMON	Detectability EASY	Impact SEVERE	Application / Business Specific
Consider anyone who	Attacker uses weak	Authentication may not be	sufficient when weak	Insufficient	Consider the business
has access to the web	passwords, insecure	passwords are used or are	e poorly protected.	authentication/authorization	impact of compromised
interface, mobile	password recovery	Insufficient authentication	authorization is prevalent	can result in data loss or	user accounts and
interface or cloud	mechanisms, poorly	as it is assumed that interfaces will only be		corruption, lack of	possibly devices. All data
interface including	protected credentials or	exposed to users on internal networks and not to		accountability, or denial of	could be stolen,
internal and external	lack of granular access	external users on other networks. Deficiencies are		access and can lead to	modified, or deleted.
users.	control to access a	often found to be present	across all interfaces.	complete compromise of	Could your customers be
	particular interface.	Many Issues with authent	cation/authorization are	the device and/or user	harmed?
	Attack could come from	easy to discover when examining the interface		accounts.	
	external or internal	manually and can also be	discovered via		
	users.	automated testing.			





### I2 | Insufficient Authentication/Authorization | Testing

#### Is My Authentication/Authorization Sufficient?

Checking for Insufficient Authentication includes:

- Attempting to use simple passwords such as "1234" is a fast and easy way to determine if the password policy is sufficient across all interfaces
- Reviewing network traffic to determine if credentials are being transmitted in clear text
- Reviewing requirements around password controls such as password complexity, password history check, password expiration and forced password reset for new users
- Reviewing whether re-authentication is required for sensitive features

Checking for Insufficient Authorization includes:

- Reviewing the various interfaces to determine whether the interfaces allow for separation of roles. For example, all features will be accessible to administrators, but users will have a more limited set of features available.
- · Reviewing access controls and testing for privilege escalation
  - Lack of Password Complexity
  - Poorly Protected Credentials
  - Lack of Two Factor Authentication
  - Insecure Password Recovery
  - Privilege Escalation
  - Lack of Role Based Access Control

#### **Example Attack Scenarios**

Scenario #1: The interface only requires simple passwords.

```
Username = Bob; Password = 1234
```

**Scenario #2:** Username and password are poorly protected when transmitted over the network.

```
Authorization: Basic YWRtaW46MTIzNA==
```

In the cases above, the attacker is able to either easily guess the password or is able to capture the credentials as they cross the network and decode it since the credentials are only protected using Base64 Encoding.





### How Do I Make My Authentication/Authorization Better?

Sufficient authentication/authorization requires:

- 1. Ensuring that the strong passwords are required
- 2. Ensuring granular access control is in place when necessary
- 3. Ensuring credentials are properly protected
- 4. Implement two factor authentication where possible
- 5. Ensuring that password recovery mechanisms are secure
- 6. Ensuring re-authentication is required for sensitive features
- 7. Ensuring options are available for configuring password controls

Please review the following tabs for more detail based on whether you are a Manufacturer  ${}_{\vec{G}}$ , Developer  ${}_{\vec{G}}$  or Consumer  ${}_{\vec{G}}$ 





# I3 | Insecure Network Services

Threat Agents	Attack Vectors	Security Weakness		Technical Impacts	Business Impacts
Application Specific	Exploitability AVERAGE	Prevalence UNCOMMON	Detectability AVERAGE	Impact MODERATE	Application / Business Specific
Consider anyone who has	Attacker uses vulnerable	Insecure network services	may be susceptible to	Insecure network services	Consider the business
access to the device via a	network services to attack	buffer overflow attacks or a	attacks that create a denial	can result in data loss or	impact of devices which
network connection,	the device itself or bounce	of service condition leaving	the device inaccessible	corruption, denial of	have been rendered
including external and	attacks off the device.	to the user. Denial of servi	ce attacks against other	service or facilitation of	useless from a denial of
internal users.	Attack could come from	users may also be facilitate	ed when insecure network	attacks on other devices.	service attack or the
	external or internal users.	services are available. Inse	ecure network services can		device is used to facilitate
		often be detected by auton	nated tools such as port		attacks against other
		scanners and fuzzers.			devices and networks.
					Could your customers or
					other users be harmed?





## I3 | Insecure Network Services | Testing

#### Are My Network Services Secure?

Checking for Insecure Network Services includes:

- Determining if insecure network services exist by reviewing your device for open ports using a port scanner
- As open ports are identified, each can be tested using any number of automated tools that look for DoS vulnerabilities, vulnerabilities related to UDP services and vulnerabilities related to buffer overflow and fuzzing attacks
- Reviewing network ports to ensure they are absolutely necessary and if there are any ports being exposed to the internet using UPnP.

- Vulnerable Services
- Buffer Overflow
- Open Ports via UPnP
- Exploitable UDP Services
- Denial-of-Service
- DoS via Network Device Fuzzing

#### Example Attack Scenarios

Scenario #1: Fuzzing attack causes network service and device to crash.

```
GET %s%s%s%s%s%s%s%s%s%s%s%s%s%s HTTP/1.0
```

Scenario #2: Ports open to the internet possibly without the user's knowledge via UPnP.

```
Port 80 and 443 exposed to the internet via a home router.
```

In the cases above, the attacker is able to disable the device completely with an HTTP GET or access the device via the internet over port 80 and/or port 443.





### I3 | Insecure Network Services | Make It Secure

#### How Do I Secure My Network Services?

Securing network services requires:

- 1. Ensuring only necessary ports are exposed and available.
- Ensuring services are not vulnerable to buffer overflow and fuzzing attacks.
- Ensuring services are not vulnerable to DoS attacks which can affect the device itself or other devices and/or users on the local network or other networks.
- 4. Ensuring network ports or services are not exposed to the internet via UPnP for example

Please review the following tabs for more detail based on whether you are a Manufacturer &, Developer & or Consumer &





# I4 | Lack of Transport Encryption

Threat Agents	Attack Vectors	Security Weakness		Technical Impacts	Business Impacts
Application Specific	Exploitability AVERAGE	Prevalence COMMON	Detectability EASY	Impact SEVERE	Application / Business Specific
Consider anyone who has	Attacker uses the lack of	Lack of transport encryption	n allows data to be viewed	Lack of transport	Consider the business
access to the network the	transport encryption to	as it travels over local netw	orks or the internet. Lack	encryption can result in	impact of exposed data
device is connected to,	view data being passed	of transport encryption is p	revalent on local networks	data loss and depending	as it travels across
including external and	over the network. Attack	as it is easy to assume tha	t local network traffic will	on the data exposed,	various networks. Data
internal users.	could come from external	not be widely visible, howe	ver in the case of a local	could lead to complete	could be stolen or
	or internal users.	wireless network, misconfiç	guration of that wireless	compromise of the device	modified. Could your
		network can make traffic vi	sible to anyone within	or user accounts.	users be harmed by
		range of that wireless netw	ork. Many Issues with		having their data
		transport encryption are ea	sy to discover simply by		exposed?
		viewing network traffic and	searching for readable		
		data. Automated tools can	also look for proper		
		implementation of commor	transport encryption such		
		as SSL and TLS.			





### I4 | Lack of Transport Encryption | Testing

#### Do I Use Transport Encryption?

Checking for Lack of Transport Encryption includes:

- Reviewing network traffic of the device, its mobile application and any cloud connections to determine if any information is passed in clear text
- Reviewing the use of SSL or TLS to ensure it is up to date and properly implemented
- Reviewing the use of any encryption protocols to ensure they are recommended and accepted

- Unencrypted Services via the Internet
- Unencrypted Services via the Local Network
- Poorly Implemented SSL/TLS
- Misconfigured SSL/TLS

#### **Example Attack Scenarios**

Scenario #1: The cloud interface uses only HTTP.

```
http://www.xyzcloudsite.com
```

**Scenario #2:** Username and password are transmitted in the clear over the network.

```
http://www.xyzcloud.com/login.php?userid=3&
password=1234
```

In the cases above, the attacker has the ability to view sensitive data in the clear due to lack of transport encryption.





### I4 | Lack of Transport Encryption | Make It Secure

#### How Do I Use Transport Encryption?

Sufficient transport encryption requires:

- 1. Ensuring data is encrypted using protocols such as SSL and TLS while transiting networks.
- 2. Ensuring other industry standard encryption techniques are utilized to protect data during transport if SSL or TLS are not available.
- Ensuring only accepted encryption standards are used and avoid using proprietary encryption protocols

Please review the following tabs for more detail based on whether you are a Manufacturer \$\vec{\vec{v}}\$, Developer \$\vec{\vec{v}}\$ or Consumer \$\vec{\vec{v}}\$





# I5 | Privacy Concerns

Threat Agents	Attack Vectors	Security Weakness		Technical Impacts	<b>Business Impacts</b>
Application Specific	Exploitability AVERAGE	Prevalence COMMON	Detectability EASY	Impact SEVERE	Application / Business Specific
itself, the network the device is connected to, the mobile application and the cloud connection including external and internal users.	vectors such as insufficient authentication, lack of transport encryption or insecure network services to view personal data which is not	Privacy concerns generate personal data in addition to protection of that data is prare easy to discover by sin that is being collected as the activates the device. Autor for specific patterns of data collection of personal data	the lack of proper revalent. Privacy concerns inply reviewing the data the user sets up and inated tools can also look a that may indicate	data along with a lack of protection of that data can lead to compromise of a user's personal data.	Consider the business impact of personal data that is collected unnecessarily or isn't protected properly. Data could be stolen. Could your customers be harmed by having this personal data exposed?





# I5 | Privacy Concerns | Testing

#### Does My Device Present Privacy Concerns?

Checking for Privacy Concerns includes:

- Identifying all data types that are being collected by the device, its mobile app and any cloud interfaces
- The device and it's various components should only collect what is necessary to perform its function
- Personally identifiable information can be exposed when not properly encrypted while at rest on storage mediums and during transit over networks
- Reviewing who has access to personal information that is collected

 Collection of Unnecessary Personal Information

#### **Example Attack Scenarios**

Scenario #1: Collection of personal data.

Date of birth, home address, phone number, etc.

Scenario #2: Collection of financial and/or health information.

Credit card data and bank account information.

In the cases above, exposure of any of the data examples could lead to identity theft or compromise of accounts.





# I5 | Privacy Concerns | Make It Secure

#### How Do I Prevent Privacy Concerns?

Minimizing privacy concerns requires:

- 1. Ensuring only data critical to the functionality of the device is collected
- 2. Ensuring any data collected is properly protected with encryption
- 3. Ensuring the device and all of its components properly protect personal information
- 4. Ensuring only authorized individuals have access to collected personal information

Please review the following tabs for more detail based on whether you are a Manufacturer, Developer or Consumer





# I6 | Insecure Cloud Interface

Threat Agents	Attack Vectors	Security Weakness		Technical Impacts	Business Impacts
Application Specific	Exploitability AVERAGE	Prevalence COMMON	Detectability EASY	Impact SEVERE	Application / Business Specific
Consider anyone who	Attacker uses multiple	An insecure cloud interfac	e is present when easy to	An insecure cloud	Consider the business
has access to the	vectors such as	guess credentials are used	d or account enumeration	interface could lead to	impact of an insecure
internet.	insufficient	is possible. Insecure cloud	is possible. Insecure cloud interfaces are easy to		cloud interface. Data
	authentication, lack of	discover by simply reviewi	ng the connection to the	and control over the	could be stolen or
	transport encryption and	cloud interface and identify	ying if SSL is in use or by	device.	modified and control over
	account enumeration to	using the password reset i	mechanism to identify		devices assumed. Could
	access data or controls	valid accounts which can I	ead to account		your customers be
	via the cloud website.	enumeration.			harmed? Could your
	Attack will most likely				brand be harmed?
	come from the internet.				





# I6 | Insecure Cloud Interface | Testing

#### Is My Cloud Interface Secure?

Checking for a Insecure Cloud Interface includes:

- Determining if the default username and password can be changed during initial product setup
- Determining if a specific user account is locked out after 3 5 failed login attempts
- Determining if valid accounts can be identified using password recovery mechanisms or new user pages
- Reviewing the interface for issues such as cross-site scripting, cross-site request forgery and sql injection.
- Reviewing all cloud interfaces for vulnerabilities (API interfaces and cloud-based web interfaces)

- Account Enumeration
- No Account Lockout
- Credentials Exposed in Network Traffic

#### **Example Attack Scenarios**

Scenario #1: Password reset indicates whether account is valid.

Password Reset "That account does not exist."

**Scenario #2:** Username and password are poorly protected when transmitted over the network.

Authorization: Basic S2ZjSDFzYkF4ZzoxMjM0NTY3

In the cases above, the attacker is able to either determine a valid user account or is able to capture the credentials as they cross the network and decode them since the credentials are only protected using Base64 Encoding.





### I6 | Insecure Cloud Interface | Make It Secure

#### How Do I Secure My Cloud Interface?

A secure cloud interface requires:

- Default passwords and ideally default usernames to be changed during initial setup
- 2. Ensuring user accounts can not be enumerated using functionality such as password reset mechanisms
- 3. Ensuring account lockout after 3- 5 failed login attempts
- Ensuring the cloud-based web interface is not susceptible to XSS, SQLi or CSRF
- 5. Ensuring credentials are not exposed over the internet
- 6. Implement two factor authentication if possible

Please review the following tabs for more detail based on whether you are a Manufacturer \$\varPi\$, Developer \$\varPi\$ or Consumer \$\varPi\$





# I7 | Insecure Mobile Interface

Threat Agents	Attack Vectors	Security Weakness		Technical Impacts	Business Impacts
Application Specific	Exploitability AVERAGE	Prevalence COMMON	Detectability EASY	Impact SEVERE	Application / Business Specific
Consider anyone who has	Attacker uses multiple	An insecure mobile interfac	ce is present when easy to	An insecure mobile	Consider the business
access to the mobile	vectors such as	guess credentials are used	d or account enumeration	interface could lead to	impact of an insecure
application.	insufficient authentication,	is possible. Insecure mobil	e interfaces are easy to	compromise of user data	mobile interface. Data
	lack of transport	discover by simply reviewing	ng the connection to the	and control over the	could be stolen or
	encryption and account	wireless networks and ider	wireless networks and identifying if SSL is in use or		modified and control over
	enumeration to access	by using the password res	et mechanism to identify		devices assumed. Could
	data or controls via the	valid accounts which can lead to account			your customers be
	mobile interface.	enumeration.			harmed? Could your
					brand be harmed?





## I7 | Insecure Mobile Interface | Testing

#### Is My Mobile Interface Secure?

Checking for an Insecure Mobile Interface includes:

- Determining if the default username and password can be changed during initial product setup
- Determining if a specific user account is locked out after 3 5 failed login attempts
- Determining if valid accounts can be identified using password recovery mechanisms or new user pages
- Reviewing whether credentials are exposed while connected to wireless networks
- Reviewing whether two factor authentication options are available

- Account Enumeration
- No Account Lockout
- Credentials Exposed in Network Traffic

#### **Example Attack Scenarios**

Scenario #1: Password reset indicates whether account exist or not.

```
Password Reset "That account does not exist."
```

**Scenario #2:** Username and password are poorly protected when transmitted over the network.

```
Authorization: Basic S2ZjSDFzYkF4ZzoxMjM0NTY3
```

In the cases above, the attacker is able to either determine a valid user account or is able to capture the credentials as they cross the network and decode them since the credentials are only protected using Base64 Encoding.





### I7 | Insecure Mobile Interface | Make It Secure

#### How Do I Secure My Mobile Interface?

A secure mobile interface requires:

- Default passwords and ideally default usernames to be changed during initial setup
- 2. Ensuring user accounts can not be enumerated using functionality such as password reset mechanisms
- 3. Ensuring account lockout after an 3 5 failed login attempts
- 4. Ensuring credentials are not exposed while connected to wireless networks
- 5. Implementing two factor authentication if possible

Please review the following tabs for more detail based on whether you are a Manufacturer, Developer or Consumer





# I8 | Insufficient Security Configurability

Threat Agents	Attack Vectors	Security \	<b>W</b> eakness	Technical Impacts	Business Impacts
Application Specific	Exploitability AVERAGE	Prevalence COMMON	Detectability EASY	Impact MODERATE	Application / Business Specific
Consider anyone who	Attacker uses the lack of	Insufficient security config	urability is present when	Insufficient security	Consider the business
has access to the device.	granular permissions to	users of the device have li	mited or no ability to alter	configurability could lead	impact if data can be
	access data or controls	its security controls. Insuff	icient security	to compromise of the	stolen or modified and
	on the device. The	configurability is apparent	when the web interface of	device whether	control over the device
	attacker could also us the	the device has no options	for creating granular user	intentional or accidental	assumed. Could your
	lack of encryption options	permissions or for example	e, forcing the use of	and/or data loss.	customers be harmed?
	and lack of password	strong passwords. Manua	I review of the web		
	options to perform other	interface and its available	options will reveal these		
	attacks which lead to	deficiencies.			
	compromise of the device				
	and/or data. Attack could				
	potentially come from any				
	user of the device				
	whether intentional or				
	accidental.				





### I8 | Insufficient Security Configurability | Testing

#### Is My Security Configurability Sufficient?

Checking for Insufficient Security Configurability includes:

- Reviewing the administrative interface of the device for options to strengthen security such as forcing the creation of strong passwords
- Reviewing the administrative interface for the ability to separate admin users from normal users
- · Reviewing the administrative interface for encryption options
- Reviewing the administrative interface for options to enable secure logging of various security events
- Reviewing the administrative interface for options to enable alerts and notifications to the end user for security events

- Lack of Granular Permission Model
- Lack of Password Security Options
- No Security Monitoring
- No Security Logging

#### **Example Attack Scenarios**

Scenario #1: No ability to enforce strong password policies.

Admins and users are allowed to create passwords for their accounts.

Scenario #2: No ability to enable encryption of data at rest.

Password or other sensitive data stored on the device may not be encrypted.

In the cases above, the attacker is able to use the lack of these controls to get access to user accounts with weak passwords or access data at rest which has protection.





#### How Do I Improve My Security Configurability?

Sufficient security configurability requires:

- Ensuring the ability to separate normal users from administrative users
- 2. Ensuring the ability to encrypt data at rest or in transit
- 3. Ensuring the ability to force strong password policies
- 4. Ensuring the ability to enable logging of security events
- 5. Ensuring the ability to notify end users of security events

Please review the following tabs for more detail based on whether you are a Manufacturer , Developer or Consumer





# I9 | Insecure Software/Firmware

Threat Agents	Attack Vectors	Security Weakness		Technical Impacts	Business Impacts
Application Specific	Exploitability DIFFICULT	Prevalence COMMON	Detectability EASY	Impact SEVERE	Application / Business Specific
Consider anyone who	Attacker uses multiple	The lack of ability for a dev	vice to be updated	Insecure	Consider the business
has access to the device	vectors such as capturing	presents a security weakn	ess on its own. Devices	software/firmware could	impact if data can be
and/or the network the	update files via	should have the ability to b	be updated when	lead to compromise of	stolen or modified and
device resides on. Also	unencrypted connections,	vulnerabilities are discover	red and software/firmware	user data, control over	devices taken control of
consider anyone who	the update file itself is not	updates can be insecure v	when the updated files	the device and attacks	for the purpose of
could gain access to the	encrypted or they are	themselves and the netwo	rk connection they are	against other devices.	attacking other devices.
update server.	able to perform their own	delivered on are not protec	cted. Software/Firmware		Could your customers be
	malicious update via DNS	can also be insecure if the	y contain hardcoded		harmed? Could other
	hijacking. Depending on	sensitive data such as cre	dentials. Security issues		users be harmed?
	method of update and	with software/firmware are	relatively easy to		
	device configuration,	discover by simply inspect	ing the network traffic		
	attack could come from	during the update to check	for encryption or using a		
	the local network or the	hex editor to inspect the up	pdate file itself for		
	internet.	interesting information.			





### I9 | Insecure Software/Firmware | Testing

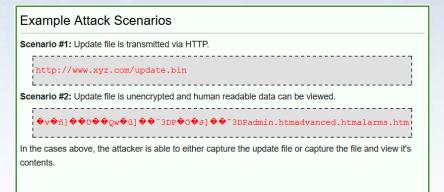
#### Is My Software/Firmware Secure?

 Note - It is very important that devices first and foremost have the ability to update and perform updates regularly.

Checking for insecure software/firmware updates include:

- Reviewing the update file itself for exposure of sensitive information in human readable format by someone using a hex edit tool
- · Reviewing the production file update for proper encryption using accepted algorithms
- · Reviewing the production file update to ensure it is properly signed
- · Reviewing the communication method used to transmit the update
- Reviewing the cloud update server to ensure transport encryption methods are up to date and properly configured and that the server itself is not vulnerable
- · Reviewing the device for proper validation of signed update files

- Encryption Not Used to Fetch Updates
- Update File not Encrypted
- Update Not Verified before Upload
- Firmware Contains Sensitive Information
- No Obvious Update Functionality







# How Do I Secure My Software/Firmware?

Securing software/firmware require:

- Ensuring the device has the ability to update (very important)
- 2. Ensuring the update file is encrypted using accepted encryption methods
- 3. Ensuring the update file is transmitted via an encrypted connection
- 4. Ensuring the update file does not contain sensitive data
- Ensuring the update is signed and verified before allowing the update to be uploaded and applied
- 6. Ensuring the update server is secure

Please review the following tabs for more detail based on whether you are a Manufacturer ♂,

Developer 🗗 or Consumer 🗗





# I10 | Poor Physical Security

Threat Agents	Attack Vectors	Security Weakness		Technical Impacts	Business Impacts
Application Specific	Exploitability AVERAGE	Prevalence COMMON	Detectability AVERAGE	Impact SEVERE	Application / Business Specific
Consider anyone who has	Attacker uses vectors	Physical security weaknesses are present when an		Insufficient physical	Data could be stolen or
physical access to the	such as USB ports, SD	attacker can disassemble a device to easily access		security could lead to	modified and the device
device.	cards or other storage	the storage medium and ar	ny data stored on that	compromise of the device	taken control of for
	means to access the	medium. Weaknesses are	also present when USB	itself and any data stored	purposes other than what
	Operating System and	ports or other external port	s can be used to access	on that device.	was originally intended.
	potentially any data	the device using features intended for configuration			Could your customers be
	stored on the device.	or maintenance.			harmed? Could your
					brand be harmed?





# I10 | Poor Physical Security | Testing

#### Is My Physical Security Sufficient?

Checking for Poor Physical Security includes:

- Reviewing how easily a device can be disassembled and data storage mediums accessed or removed
- Reviewing the use of external ports such as USB to determine if data can be accessed on the device without disassembling the device.
- Reviewing the number of physical external ports to determine if all are required for proper device function
- Reviewing the administrative interface to determine if external ports such as USB can be deactivated
- Reviewing the administrative interface to determine if administrative capabilities can be limited to local access only

- Access to Software via USB Ports
- Removal of Storage Media

#### **Example Attack Scenarios**

**Scenario #1:** The device can be easily disassembled and storage medium is an unencrypted SD card.

SD card can be removed and inserted into a card reader to be modified or copied.

Scenario #2: USB ports are present on the device.

Custom software could be written to take advantage of features such as updating via the USB port to modify the original device software.

In both cases, an attacker is able to access the original device software and make modifications or simply copy specific target data.





### I10 | Poor Physical Security | Make It Secure

#### How Do I Physically Secure My Device?

Adequate physical security requires:

- 1. Ensuring data storage medium can not be easily removed.
- 2. Ensuring stored data is encrypted at rest.
- 3. Ensuring USB ports or other external ports can not be used to maliciously access the device.
- 4. Ensuring device can not be easily disassembled.
- 5. Ensuring only required external ports such as USB are required for the product to funtion
- 6. Ensuring the product has the ability to limit administrative capabilities

Please review the following tabs for more detail based on whether you are a Manufacturer \$\vec{\vec{w}}\$, Developer \$\vec{\vec{w}}\$ or Consumer \$\vec{\vec{w}}\$





### Resources

- OWASP Internet of Things Top Ten
- <u>Email List</u>



