Security Advisory

September 2019

DDOS Attacks using WS Discovery

Sources:

- https://zero.bs/new-ddos-attack-vector-via-ws-discoverysoapoverudp-port-3702.html

Overview

An ONVIF device exposing the WS Discovery (UDP port 3702) towards the Internet could be exploited for a Distributed-Denial-Of-Service (DDOS) attack targeting 3:rd party Internet services. The attacker makes a request to the WS Discovery port 3702 with a spoofed source address (3:rd party address), making the WS Discovery respond with data to that 3:rd party service. A DDOS attack may be successful if an attacker is able to make spoofed WS Discovery requests to thousands of Internet facing devices simultaneously.

Risk assessment

The impact for the device owner is limited as the attack is not targeting the device or the system it belongs to. It is not possible to exploit WS Discovery for a public attack if the device is behind a firewall (and not exposing UDP port 3702) which is the typical case for most professional video systems. Devices discovered by search engines such as Shodan.io and BinaryEdge are at high risk. Exposed devices are in most cases a result of a DIY installations, typically belonging to small organizations such as consumers, family businesses and non-profit.

Risk mitigation

Keep devices behind a firewall and do not expose any ports. If needed, remote video access should be provided by the VMS (Video Management System) in a secure manner. Small organizations not operating a VMS are recommended to use AXIS Companion client that provides secure remote video access.

If there is an increased risk of an adversary on the internal/private/local LAN, there are some additional security controls that could be applied:

1. **IP Filtering:**
   Configuring IP filtering (IP tables) in the device will reject requests from non-whitelisted IP address. Read more the in User Manual.
2. **Disabling WS Discovery:**
   It is possible to disable WS Discovery in Axis devices. This will require technical skills. Contact Axis support.

Affected Axis products and firmware

All Axis devices that supports ONVIF are susceptible to the described attack. WS Discovery is enabled by default regardless if ONVIF API is used or not.

Axis plan

Axis is investigating modifying WS Discovery behavior to reduce risk if port 3702 is exposed. If adjustments will be made, they will be announced in a future scheduled firmware release.