View on GitHub

Advisory - Loxone Cloud DNS Vulnerability

In order to access the Loxone Miniserver from outside the home network Loxone offers the Cloud DNS service. In this service the announcement of the Loxone Miniservers' public IP address to the Cloud DNS service is unauthenticated. As a consequence an attacker can register his own IP address at the service if he knows a MAC address of a Loxone Miniserver. When running a webserver at this IP address (e.g. with a website similar to the Loxone Miniserver web interface) he is able to tap the users' credentials. With these credentials the attacker can access the Loxone Miniserver and furthermore the whole Loxone Smart Home depending on the users' permissions.

Title	**Loxone Miniserver - Loxone Cloud DNS Vulnerability**
Product	Loxone Miniserver Gen. 1
Vulnerable firmware versions	Every version before `11.1.9.3` since the introduction of Loxone Cloud DNS (confirmed by Loxone; tested with `11.0.5.5` and `10.3.11.27`)
Fixed firmware version	`11.1.9.3`
CVE-ID	CVE-2020-27488
Vendor website	https://www.loxone.com/enen/
Identified in	June 2020
Identified by	IoT Lab, University of Applied Sciences Upper Austria, Campus Hagenberg
Website	https://www.fh-ooe.at/si/
Team	Simon Birngruber BSc (University of Applied Sciences Upper Austria Campus Hagenberg) Dieter Vymazal BSc MSc (University of Applied Sciences Upper Austria Campus Hagenberg) DI Markus Zeilinger (University of Applied Sciences Upper Austria Campus Hagenberg)
Contact details	Simon Birngruber simon.birngruber@students.fh-hagenberg.at PGP Fingerprint: E013 87A8 D4CA EB69 78E6 014C A27E 5026 6149 054A

Vendor description

„We focus on the simple idea of creating a building that knows what to do on its own. From smart homes to commercial buildings of all types, our goal is that it is equipped with the truly intelligent automation for the simplest control."

Source: https://www.loxone.com/enus/about-us/mission/

Overview

As an alternative to DDNS providers like No-IP or DynDNS Loxone offers the Cloud DNS service (https://www.loxone.com/enen/kb/dns-service/). With this service customers who get assigned a dynamic public IP address from their Internet service provider can access their Loxone Miniserver through a fixed URI. The URI has the structure `http://dns.loxonecloud.com/{Miniserver-MAC}` where the string `{Miniserver-MAC}` is the serial number or respectively the MAC address of the Miniserver. Based on this URI the Cloud DNS service redirects a request through a HTTP redirect (`307 - Temporary Redirect`) to the currently registered IP address of the queried Loxone Miniserver. To enable this function port forwarding from the router to the Loxone Miniserver has to be configured in the home network of the user. The announcement of the current public IP address of the home network is done by the Loxone Miniserver. Every minute the Loxone Miniserver sends a UDP datagram to the destination port `7070` of an IP address in the resource record set `dns.loxonecloud.com`. The UDP datagram has the following structure: `504F94000000,80,01343c51,0123456789ABCDEF`

- `504F94000000` = MAC address of the Loxone Miniserver
- `80` = Port where the web interface of the Miniserver is reachable
- `01343c51` = Hexadecimal representation of the build date of the currently installed web interface on the Loxone Miniserver (in this example `01343c51` HEX = `20200529` DEC -> 29.05.2020)
- `0123456789ABCDEF` = 8 bytes hexadecimal string, meaning currently unknown, value has no visible impact and can be chosen arbitrary (except the fixed length)

Afterwards the Loxone Cloud DNS service registers the source IP address of the UDP datagram (= public IP address of the home network) and the given port as entry point for the Loxone Miniserver with the given MAC address.

The mode of operation of the Loxone Cloud DNS service is shown in Figure 1. Every minute the Loxone Miniserver sends a UDP datagram with the mentioned information to the Loxone Cloud DNS service (1). There the given information and additionally the current timestamp (in this example 01.07.2020 10:55:21) is saved (2). If a user is now calling the URI of this Loxone Miniserver (3) the request is redirected to the currently registered IP address (4) (in this example to `http://192.0.2.1:80/`). Finally the web interface is called directly from the Loxone Miniserver (5).

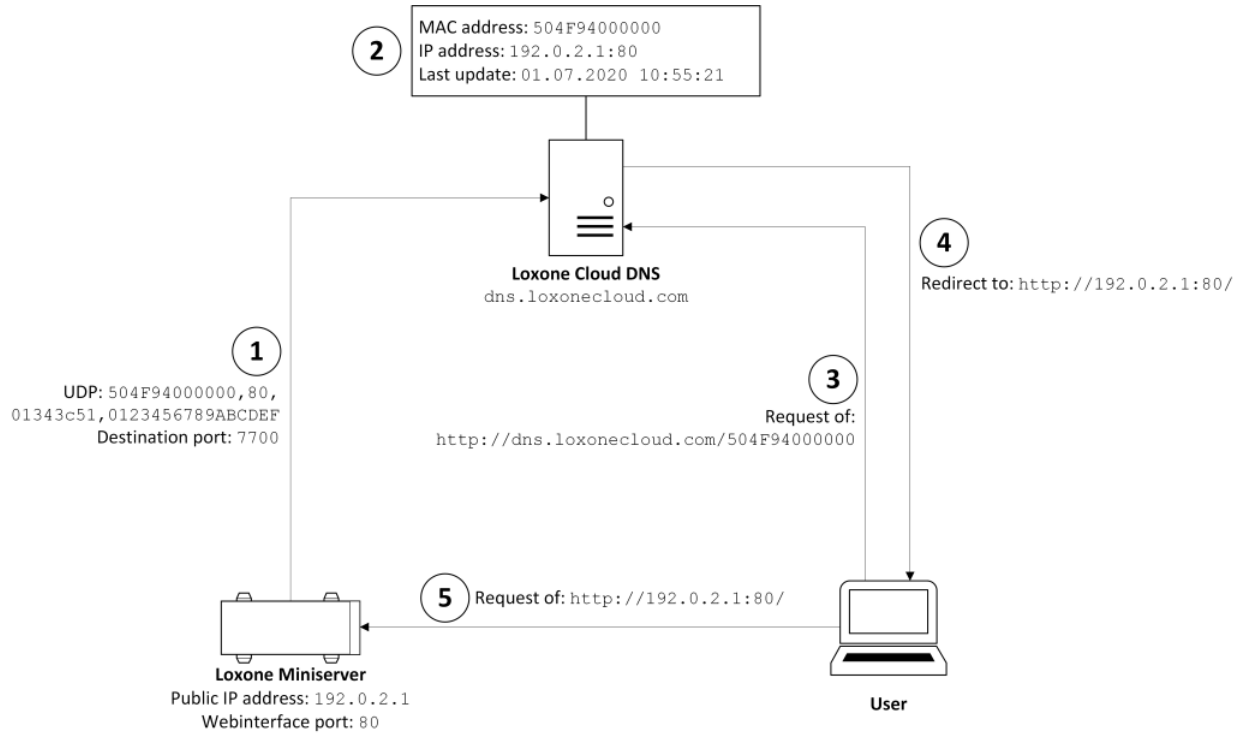

Figure 1: Mode of operation of the Loxone Cloud DNS service

Vulnerability description

In the whole process described before it is never validated whether the device which sends the UDP datagram is actually the Loxone Miniserver with the provided MAC address. Because of this missing authentication an attacker can send such UDP datagrams with any MAC address from the Loxone OUI (Organizationally Unique Identifier) `504F94`. All requests to the Loxone Cloud DNS URI are then redirected to the UDP datagram senders' public IP address. At this IP address the attacker could run a webserver with a fake version of the Miniservers' web interface and then tap the credentials of a user. Because the Loxone Miniserver isn't reachable via the URI just by changing the IP address in the Loxone Cloud DNS entry (without hosting a website) a Denial of Service from the internet is already achieved. An attack can be executed on any MAC address in the OUI range of Loxone. However without knowing the MAC address the attack can't be performed targeted to a specific Miniserver (e.g. at a specific location).

Proof of Concept

The following assumptions are made for the proof of concept:

- MAC address of the Loxone Miniserver: `504F94000000`
- Public IP address of the home network where the Loxone Miniserver is located: `192.0.2.1`
- Public IP address of the attacker: `192.0.2.2`
- Port of the Loxone Miniservers' web interface: `80`
- Port of the attackers' fake web interface: `8080`
- Build date of the installed web interface in hexadecimal representation (29.05.2020): `01343c51`
- 8 bytes hexadecimal string: `0123456789ABCDEF`

The in the following described procedure is illustrated simplified in Figure 2.

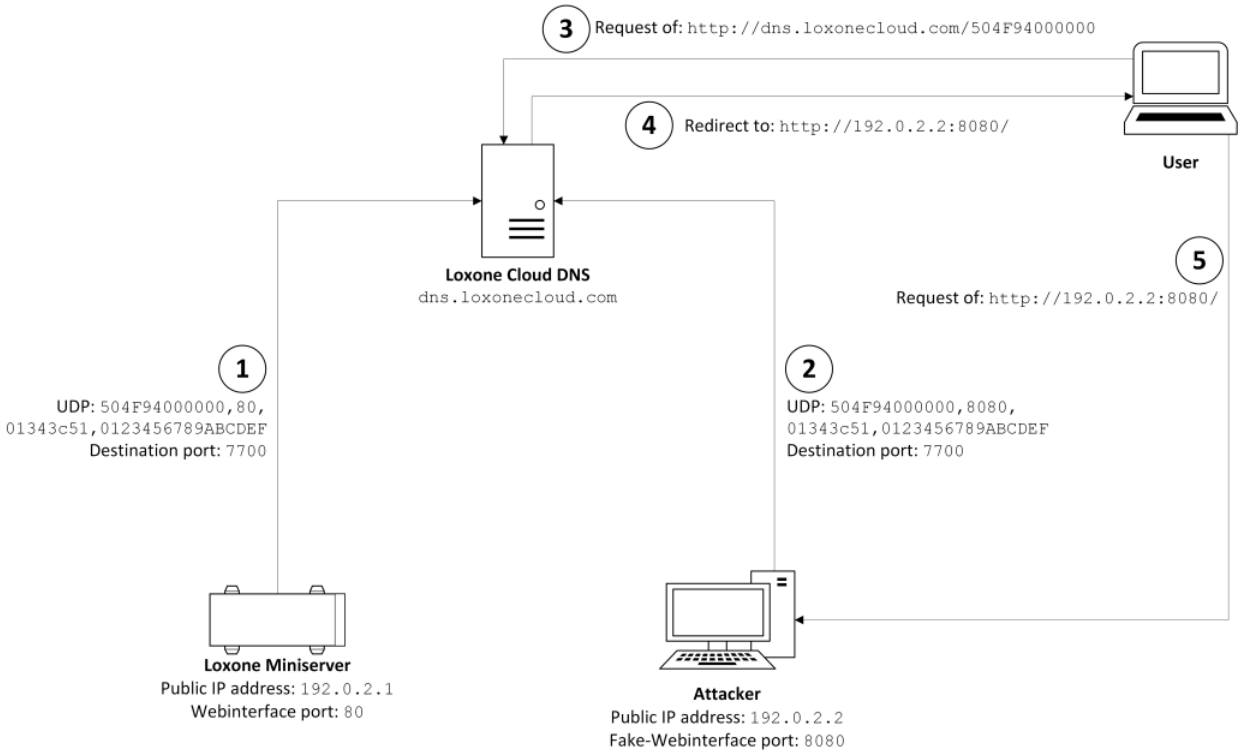

Figure 2: Proof of Concept

At first the Loxone Miniserver has to be registered at Loxone and the Loxone Cloud DNS service has to be enabled via Loxone Config. Afterwards the Loxone Miniserver starts sending UDP datagrams as described in "Overview" (1). Thus the public IP address of the Loxone Miniserver (`192.0.2.1`) and the port of the web interface (`80`) are stored at the Loxone Cloud DNS service. An attacker can now send UDP datagrams containing the MAC address of the corresponding Loxone Miniserver (2). After the UDP datagram is sent by the attacker the IP address and the port of the Loxone Cloud DNS entry are changed to `192.0.2.2` and `8080` in this example. If a request of the URI `http://dns.loxonecloud.com/504F94000000` occurs from a user after this change (3), the Loxone Cloud DNS service redirects the request to the attackers' webserver at `http://192.0.2.2:8080` (4, 5). At this webserver the attacker is hosting a copy of the Loxone Miniservers' web interface (example in Figure 3) where the credentials of the user are tapped.

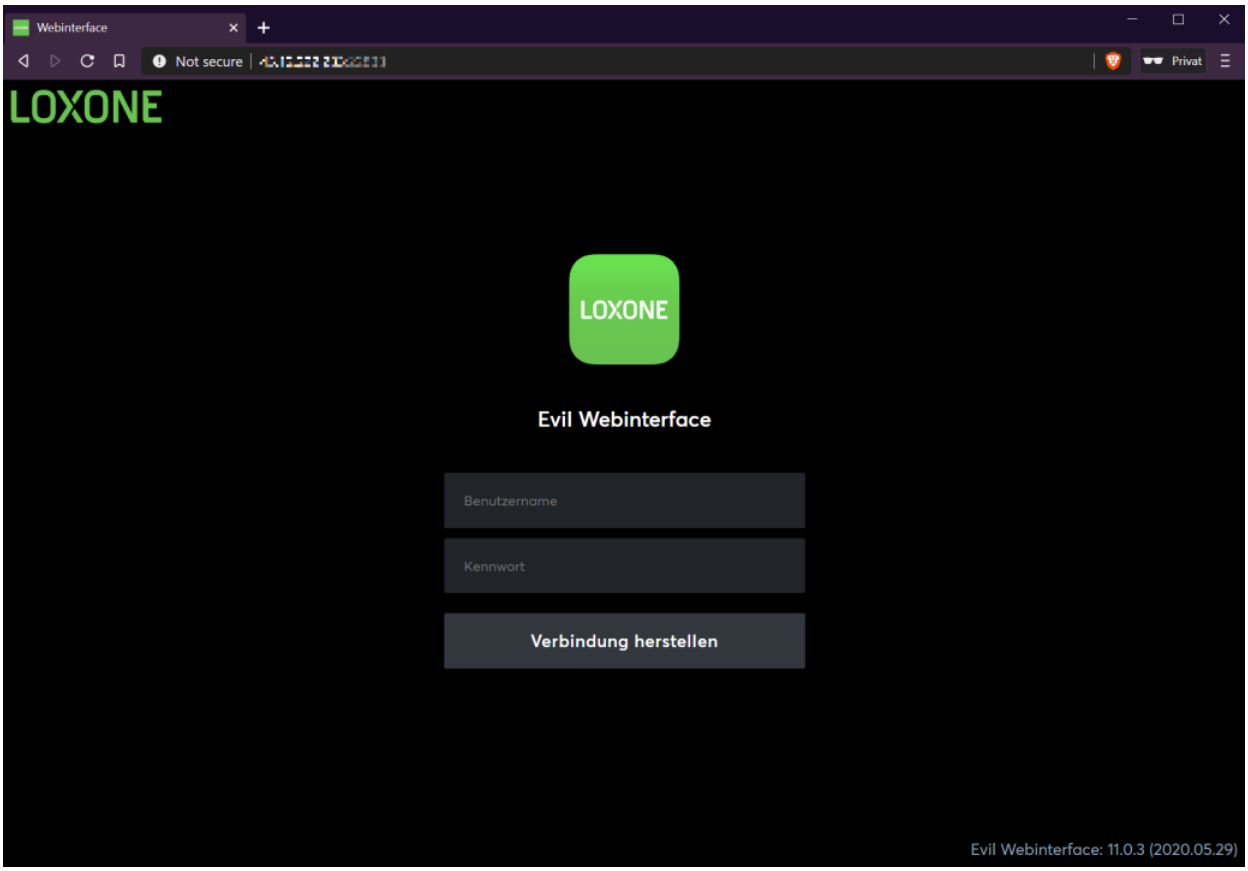

Figure 3: Evil web interface

Since the Loxone Miniserver sends a UDP datagram about every 60 seconds, the fake entry from the attacker gets overwritten at the latest after this time frame. An attacker can get useful information about the specific Loxone Miniserver through the URI `http://dns.loxonecloud.com/?getip&snr={Miniserver-MAC}&json=true`, which is mentioned in the interface description by Loxone (https://www.loxone.com/enen/kb/api/). Among other things these are the currently registered IP address and the timestamp of the last update. The attacker can therefore gather the timestamp of the last UDP datagram and can send his fake UDP datagram shortly after this time. Therefore the authentic entry is active just for a short period of time and gets overwritten by the fake entry until the next datagram from the actual Miniserver arrives. An attacker can automate this process to achieve that the authentic entry is registered in the Loxone Cloud DNS service as short as possible.

Vulnerable firmware versions

With the Proof of Concept the vulnerability was verified with a Loxone Miniserver Gen. 1 with the firmware versions `10.3.11.27` and `11.0.5.5`. According to Loxone all firmware versions before `11.1.9.3` since the introduction of the Loxone Cloud DNS service are affected by the vulnerability.

Workaround

To prevent the exploitation of the vulnerability the Loxone Cloud DNS service has to be disabled.

Solution

Loxone published firmware version `11.1.9.3` on the 3rd of September 2020 and therefore within the public disclosure deadline. According to Loxone the vulnerability is fixed by this firmware.

Measures taken - statement Loxone

On September 29th, 2020 Loxone sent the following statement which describes the measures taken to fix the vulnerability:

1. With an HTTP request, the IP address and the port of the Miniserver, that is configured on the home router can be read (this is used by the app for external/remote access, for example). In the HTTP response, the field for “Last Update Timestamp” has been removed so as not to reveal the update cycle of the Miniserver. This measure was implemented on 6 July 2020.
2. A sophisticated check detects potential attackers as soon as the IP address changes several times within one minute. Therefore, a potential attack can be identified after a one occurence and, as a result, the IP address of the perceived attacker is then blacklisted for 24 hours. This measure was implemented on 16 July 2020.
3. Seperate to this, a single IP address can send a maximum of 50 updates to the Loxone Cloud DNS within one minute. Should this be exceeded, the IP address in this instance is blacklisted for 7 hours and all updates will simply be ignored during this time. This measure was implemented on 16 July 2020.
4. From one IP address for a Miniserver, a maximum of 5 updates per minute can be sent to the Loxone Cloud DNS. This, in itself, is to prevent update spamming for a Miniserver. Should this be exceeded, the IP address is blacklisted for 7 hours. This measure was implemented on 16 July 2020.
5. For all Minsiervers using version 11.1 (2020.09.03) and above, and which make use of the Loxone Cloud DNS, a signature of the update package was introduced. With the help of an authentication handshake, an assurance is made that the respective package originates from the Miniserver in question. Once a successful update has been carried out using this authentication method, the Miniserver will not allow any future packets that are not signed in this way. This update was rolled out to consumers and Loxone Partners on 3 September 2020.

These measures taken with the Loxone Cloud DNS ensure a strong level of protection for Loxone installations which make use of this service. We always recommend to keep installations up-to-date to benefit from such improvements. The updates in V11.1 prevent attacks based on the scenarios outlined above and therefore provide utmost protection in this regard.

Note: The attack scenarios detailed above are in reference to the Loxone DNS service only. The “Loxone Remote Connect” service is not affected by the aforementioned.

Communication timeline

Date	Sender	Description
01.07.2020	Simon Birngruber	Contacted Loxone
03.07.2020	Loxone	Request to send the advisory
04.07.2020	Simon Birngruber	Sent the advisory to Loxone and communicated our 90 day public disclosure policy
23.07.2020	Simon Birngruber	Asked about the receipt of the advisory
24.07.2020	Loxone	Confirmed the receipt of the advisory and informed about a planned firmware update
02.08.2020	Simon Birngruber	Coordination of the publication
10.08.2020	Loxone	Coordination of the publication
11.08.2020	Simon Birngruber	Coordination of the publication
11.08.2020	Loxone	Coordination of the publication

Date	Sender	Description
03.09.2020	-	Release of firmware `11.1.9.3` by Loxone
22.09.2020	Loxone	Coordination of the publication
23.09.2020	Simon Birngruber	Coordination of the publication; Request for a conference call to clarify technical details and coordinate the publication
25.09.2020	Loxone	Coordination of the publication; Confirmed conference call
25.09.2020	Simon Birngruber	Coordination of the publication
28.09.2020	-	Conference call to clarify technical details and coordinate the publication
29.09.2020	Loxone	Sent the statement for the advisory
01.10.2020	Simon Birngruber	Sent the latest version of the advisory
01.10.2020	Loxone	Comments on the advisory
02.10.2020	Simon Birngruber	Feedback on the comments
02.10.2020	Loxone	Request for adjusting the statement
05.10.2020	Loxone	Clarification of a technical detail
06.10.2020	Simon Birngruber	Sent the latest version of the advisory; Asked for an English version of the statement
06.10.2020	Loxone	Sent the English version of the statement; Coordination of the publication
08.10.2020	-	Public disclosure of the German advisory on GitHub
21.10.2020	-	Public disclosure of the English advisory on GitHub

Version history

Date	Version	Changes
21.10.2020	v1.0	Initial version of the English advisory
14.01.2021	v1.1	Added CVE-ID

Advisory - Loxone Cloud DNS Vulnerability maintained by IoT-Lab-FH-OOE

Published with GitHub Pages