Security Incident Management

Incident reported by: BSI	***Date:*** 20.01.2021
Referenced Documents: BSI-2021-20210120_v1.0_CV_TLPGREEN.pdf	
Incidents covered by this document: • Vulnerability SIM#2021-01-a: "Possible DNS cache poisoning" • Vulnerability SIM#2021-01-b: "Possible DNS cache poisoning" • Vulnerability SIM#2021-01-c: "Possible DNS cache poisoning"	
VDE-ID: VDE-2021-012	

Public disclosure:	***Date:***
Incident-Report - SIM#2021-01	26.04.2021
mbNET/mbNET.rokey Firmware 7.0.0	25.02.2021
mbNET HW1 Firmware 5.1.11	31.03.2021

ⓘ The MB connect line security team can be reached via email at security-team@mbconnectline.com. For incident-reports, please use encypted communication only. For details and PGP-credentials visit https://www.mbconnectline.de/de/support/sicherheitshinweise.html.

More information on current threats and the associated product safety of our devices and software solutions can be found at https://www.mbconnectline.de/de/support/sicherheitshinweise.html.

All vulnerability-metrics used in this document are created with the NIST NVD CVSS-Calculator V3 https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator

Vulnerability SIM#2021-01-a: "Possible DNS cache poisoning"

Details

CVE: CVE-2020-25684
Description: A flaw was found in dnsmasq before version 2.83. When getting a reply from a forwarded query, dnsmasq checks in the forward.c:reply_query() if the reply destination address/port is used by the pending forwarded queries. However, it does not use the address/port to retrieve the exact forwarded query, substantially reducing the number of attempts an attacker on the network would have to perform to forge a reply and get it accepted by dnsmasq. This issue contrasts with RFC5452, which specifies a query's attributes that all must be used to match a reply. This flaw allows an attacker to perform a DNS Cache Poisoning attack. If chained with CVE-2020-25685 or CVE-2020-25686, the attack complexity of a successful attack is reduced. The highest threat from this vulnerability is to data integrity.
Solution: Update to latest available firmware.

Affected Products

Product:	***Version:***	***Update:***
mbNET/mbNET.rokey	<= 6.2.5	7.0.0
mbNET HW1	<= 5.1.10	5.1.11

CVSS Scores & Vulnerability

CWE-Identifier:	CWE-358
CVSS Base Score:	3.7
CVSS v3 Link:	AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N

Vulnerability SIM#2021-01-b: "Possible DNS cache poisoning"

Details

CVE: CVE-2020-25685
Description: A flaw was found in dnsmasq before version 2.83. When getting a reply from a forwarded query, dnsmasq checks in forward.c:reply_query(), which is the forwarded query that matches the reply, by only using a weak hash of the query name. Due to the weak hash (CRC32 when dnsmasq is compiled without DNSSEC, SHA-1 when it is) this flaw allows an off-path attacker to find several different domains all having the same hash, substantially reducing the number of attempts they would have to perform to forge a reply and get it accepted by dnsmasq. This is in contrast with RFC5452, which specifies that the query name is one of the attributes of a query that must be used to match a reply. This flaw could be abused to perform a DNS Cache Poisoning attack. If chained with CVE-2020-25684 the attack complexity of a successful attack is reduced. The highest threat from this vulnerability is to data integrity.
Solution: Update to latest available firmware.

Affected Products

Product:	*Version:*	*Update:*
mbNET/mbNET.rokey	<= 6.2.5	7.0.0
mbNET HW1	<= 5.1.10	5.1.11

CVSS Scores & Vulnerability

CWE-Identifier:	CWE-358
CVSS Base Score:	3.7
CVSS v3 Link:	AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N

Vulnerability SIM#2021-01-c: "Possible DNS cache poisoning"

Details

CVE: CVE-2020-25686
Description: A flaw was found in dnsmasq before version 2.83. When receiving a query, dnsmasq does not check for an existing pending request for the same name and forwards a new request. By default, a maximum of 150 pending queries can be sent to upstream servers, so there can be at most 150 queries for the same name. This flaw allows an off-path attacker on the network to substantially reduce the number of attempts that it would have to perform to forge a reply and have it accepted by dnsmasq. This issue is mentioned in the "Birthday Attacks" section of RFC5452. If chained with CVE-2020-25684, the attack complexity of a successful attack is reduced. The highest threat from this vulnerability is to data integrity.
Solution: Update to latest available firmware.

Affected Products

Product:	***Version:***	***Update:***
mbNET/mbNET.rokey	<= 6.2.5	7.0.0
mbNET HW1	<= 5.1.10	5.1.11

CVSS Scores & Vulnerability

CWE-Identifier:	CWE-358, CWE-290
CVSS Base Score:	3.7
CVSS v3 Link:	AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N