Security Advisory HG-2021-001
Multiple vulnerabilities in a TCP/IP stack (InterNiche v3.1) leading to a potential denial of service in Daitem / Hager / Diagral products

Date: 04.08.2021
Version: 1.0.0

Summary

Security researchers have informed Hager of multiple vulnerabilities in InterNiche TCP/IP stack below version 4.3. These vulnerabilities could cause a denial of service. Multiple home security products implement InterNiche version 3.1, which is vulnerable. The brands concerned are Diagral, Daitem and Hager.

Upon receiving technical details, Hager has validated these vulnerabilities, which present low and limited risks to its systems, its customers, and their data. The vulnerabilities do not affect the core functionality of the alarm system. This was confirmed through testing and code review.

Hager is currently developing a new firmware to upgrade InterNiche to the latest available version (version 4.3) to remediate these issues. This update is in development as part of a bigger functional update, with a release date planned for Q1-2022.

Hager will inform its customers of the update via the usual communication channels:
- A notification on the mobile application for over-the-air update;
- A communication to installers where manual product update is required.

At the time of this publication, Hager is not aware of any exploitation of the reported vulnerabilities in its products.

Our users can protect their affected systems from successful exploitation by following the temporary counter-measures and by deploying the corrective update when available.

Products affected and risks identified

Hager has identified two product ranges implementing InterNiche TCP/IP stack in version 3.1:
- **IP alarm & control box**: stand-alone network connectivity boxes for home security systems;
- **IP plug and IP transmitter**: plug-in modules for home security systems.

Hager has validated the applicability of reported vulnerabilities. For more information on the affected products references, please refer to the reference table below.

The affected products enable an IP interface for alarm systems, allowing smartphone applications (push notification, remote monitoring), as well as the transmission of alerts and video feeds for telemonitoring. A successful exploitation can lead to denial of service with a loss of connected functionalities (loss of notification, e-mail, call) and the impossibility for the affected users to

connect to their system remotely via the smartphone application. In case of telemonitoring, the remote monitor will detect unavailability immediately and will inform the customer.

The core functionality of the alarm is not modified. This was confirmed through testing and code review.

Hager performed a risk analysis and assessed a low risk to the affected systems, its customers and their data:

- The affected products do not store nor process customer data (*e.g.* personal information, alarm code);
- The interfaces have no ability to send commands to the alarm system;
- The affected products do not execute any code from the RAM. The RAM is only used to store data. The code is directly executed from the microprocessor flash memory;
- There is no possibility to access end-user video remotely.

References of the affected products:

Several versions of these products exist under the brands Daitem, Diagral and Hager:

Model number	Brand	Description
SH501AX-1	Daitem	PSTN + IP plug-in module
SH504AX-1	Daitem	IP plug-in + Mains power supply module
SA501AX	Daitem	PSTN + IP plug-in module
SA502AX1	Daitem	GSM / GPRS + IP plug-in module
SA504AX	Daitem	IP plug-in + Mains power supply module
SH501AX	Daitem	PSTN + IP plug-in module
SH502AX2	Daitem	GSM / GPRS + IP plug-in module
SH502AX3	Daitem	GSM / GPRS + IP plug-in module
SH503AX2	Daitem	PSTN + GSM / GPRS + IP plug-in module
SH503AX3	Daitem	PSTN + GSM / GPRS + IP plug-in module
SH504AX	Daitem	IP plug-in + Mains power supply module
SH504AX1	Daitem	IP plug-in + Mains power supply module
SK501AT	Daitem	IP / ADSL connectivity box
SH501AX1	Daitem	PSTN + IP plug-in module
BH512AX	Daitem	GSM/GPRS + IP stand-alone transmitter
SA502AX	Daitem	GSM / GPRS + IP plug-in module
SH502AX	Daitem	GSM / GPRS + IP plug-in module
SH502AX1	Daitem	GSM / GPRS + IP plug-in module
SH503AX	Daitem	PSTN + GSM / GPRS + IP plug-in module
SH503AX1	Daitem	PSTN + GSM / GPRS + IP plug-in module
BH513AX	Daitem	PSTN + GSM/GPRS + IP stand-alone transmitter
BH512AX1	Daitem	GSM/GPRS + IP stand-alone transmitter
BH511AX	Daitem	PSTN + IP stand-alone transmitter
BH511AX1	Daitem	PSTN + IP stand-alone transmitter
SH511AX	Daitem	PSTN + IP stand-alone Transmitter

Model number	Brand	Description
SH512AX	Daitem	GSM/GPRS + IP stand-alone Transmitter
SH513AX	Daitem	PSTN + GSM/GPRS + IP stand-alone Transmitter
SH514AX	Daitem	IP Stand-alone Tx with mains PSU
DIAG56AAX	Diagral	IP alarm & control box
DIAG56AAX1	Diagral	IP alarm & control box
DIAG56AAX2	Diagral	IP alarm & control box
RLD002T	Hager	Hager IP/ADSL Connectivity box

Remediation

Hager will integrate the latest available version of InterNiche (v4.3) to remediate the reported vulnerabilities in a future functional update and publish a firmware update (patch).

We estimate the availability of this update in Q1-2022 following the normal validation and testing path.

Hager will inform all customers of this update through usual channels:

- Via a push on the mobile application (with the possibility to update the system);
- Through a publication on our website and mailing list for product installers (for manual product upgrade).

All our updates are provided free of charge.

Counter-measures

The core functionality of the alarm system is not affected by these vulnerabilities.

In the event of a successful exploitation, the product will lose connectivity. The main counter-measure is to restart/reboot the product directly. In some case, a reconfiguration may be necessary.

A watchdog is present that will restart the service in the most cases of service loss. In case of telemonitoring, the remote monitor will immediately notice the loss of service and will inform the customer.

List of Vulnerabilities

The affected products contain the following vulnerabilities. Hager has verified these findings through testing and code review: exploitation remains very unlikely with minimal risks on our users, their data and their systems.

For more information, please refer to the references, including technical reports from the reporters.

Note: One reported vulnerability concerns the InterNiche TFTP server. Hager products do not implement InterNiche TFTP server and remain safe from any exploitation of this particular vulnerability.

CVE-2020-25928 **The routine for parsing DNS responses does not check the "response data length" field of individual DNS answers, which may cause Out-of-Bound-Read and -Write.**
CVSS v3.1 score: 9.8 (N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)
CWE-130: Improper Handling of Length Parameter Inconsistency

CVE-2021-31226 **A heap buffer overflow exists in the code that parses the HTTP POST request due to lack of size validation.**
CVSS v3.1 score: 9.1 (AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:H)
CWE-20: Improper Input Validation

CVE-2020-25927 **The routine for parsing DNS responses does not check whether the number of queries/responses specified in the packet header corresponds to the query/response data available in the DNS packet, leading to Out-of-Bound-Read.**
CVSS v3.1 score: 8.2. (AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:H)
CWE-130: Improper Handling of Length Parameter Inconsistency

CVE-2020-25767 **The routine for parsing DNS domain names does not check whether a compression pointer points within the bounds of a packet, which leads to Out-of-Bound-Read.**
CVSS v3.1 score: 7.5 (AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)
CWE-466: Return of Pointer Value Outside of Expected Range

CVE-2020-35683 **The code that parses ICMP packets relies on an unchecked value of the IP payload size (extracted from the IP header) to compute the ICMP checksum. When the IP payload size is set to be smaller than the size of the IP header, the ICMP checksum computation function may read out of bounds.**
CVSS v3.1 score: 7.5 (AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)
CWE-20: Improper Input Validation

CVE-2020-35684 **The code that parses TCP packets relies on an unchecked value of the IP payload size (extracted from the IP header) to compute the length of the TCP payload within the TCP checksum computation function. When the IP payload size is set to be smaller than the size of the IP header, the TCP checksum computation function may read out of bounds. A low-impact write-out-of-bounds is also possible.**
CVSS v3.1 score: 7.5 (AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)
CWE-20: Improper Input Validation

CVE-2020-35685 **TCP Initial Sequence Number (ISN) are generated in a predictable manner.**
CVSS v3.1 score: 7.5 (AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N)
CWE-330: Use of Insufficiently Random Values

CVE-2021-27565 **Whenever an unknown HTTP request is received, a panic is invoked.**
CVSS v3.1 score: 7.5 (AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)
CWE-703: Improper Check or Handling of Exceptional Conditions

CVE-2021-31227 **A heap buffer overflow exists in the code that parses the HTTP POST request due to an incorrect signed integer comparison.**
CVSS v3.1 score: 7.5 (AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N)
CWE-839: Numeric Range Comparison Without Minimum Check

CVE-2021-31400 **The TCP out of band urgent data processing function would invoke a panic function if the pointer to the end of the out of band urgent data points out of the TCP segment's data. If the panic function hadn't a trap invocation removed it will result in an infinite loop and therefore a DoS (continuous loop or a device reset).**
CVSS v3.1 score: 7.5 (AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N)
CWE-248: Uncaught Exception

CVE-2021-31401 **The TCP header processing code doesn't sanitize the length of the IP length (header + data). With a crafted IP packet an integer overflow would occur whenever the length of the IP data is calculated by subtracting the length of the header from the length of the total IP packet.**
CVSS v3.1 score: 7.5 (AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N)
CWE-20: Improper Input Validation

CVE-2020-25926 **The DNS client does not set sufficiently random transaction IDs.**
CVSS v3.1 score: 4 (AV:N/AC:H/PR:N/UI:N/S:C/C:N/I:L/A:N)
CWE-330: Use of Insufficiently Random Values

CVE-2021-31228 **Attackers can predict the source port of DNS queries to send forged DNS response packets that will be accepted as valid answers to the DNS client's request.**
CVSS v3.1 score: 4 (AV:N/AC:H/PR:N/UI:N/S:C/C:N/I:L/A:N)
CWE-340: Generation of Predictable Numbers or Identifiers

Acknowledgements

Hager acknowledges BSI (bsi.bund.de) for their help and support throughout the coordination process of this vulnerability disclosure.

References

- CERT/CC Meta Advisory: https://kb.cert.org/vuls/id/608209
- HCC advisory page: https://www.hcc-embedded.com/support/security-advisories
- Forescout technical report: https://www.forescout.com/research-labs/infrahalt/
- VDOO technical report: [To complete]

Contact

Hager encourages the responsible disclosure of vulnerabilities via the dedicated email address productsecurity@hager.com.

The product security team is responsible for managing vulnerabilities found in connected product or service manufacturers and distributed by Hager Group and its companies.

Security at Hager: Cybersecurity technical and organizational measures for connected products and services

The Hager Group pays special attention to safeguard the data and connection for its digital products and services. We utilize a large framework of state of the art technical and organizational measures to achieve a secure processing of your data and provide **security**, **privacy** and **protection** of your data guided by a global IT security policy.

For connected products and services, HAGER's IT Security is inspired by the IEC-62443 standards family, which defines how to enforce IT Security for Industrial Automation and Control Systems (IACS).

HAGER provides an appropriate level of security and resilience to its product to ensure operational performance over time:

- Security updates over the cloud services are offering a fast and efficient patch management mechanism for IoT endpoints
- Vulnerability management for the centralized cloud based services
- Continuous monitoring of the systems to prevent or react quickly on unexpected events
- An IT Security incident management is offered over a professional support in case of data breach over each market segment organization (Privileged Customer Touchpoint).

More details are available on the Hager Group web site. (www.hagergroup.com)

Other information

Version: 1.0.0
Canonical URL: [URL of the advisory on Hager website]

Document history

#	Author	Date	Changes/Remarks
1.0.0	Hager Group Product Security Team	04.08.2021	Initial publication