Connecting things Hongdian

Connecting things Hongdian

Product Security Advisory

March 10,2025

Overview

Hongdian has confirmed the vulnerabilities affecting the Router application version V7.2.3_SE and prior, and has released firmware security update V7.2.5_SE, which addresses 13 security issues including CVE-2016-2183, CVE-2023-49261, CVE-2023-49259, CVE-2023-49257, etc. If you feel that your version requires additional protection, please contact your sales and technical support to update this firmware.

Details

This section summarizes the potential impact that this security update addresses.

CVE IDs	Summary	Base Score	Vector
CVE-2016-2183	The DES and Triple DES ciphers, as used in the TLS, SSH, and IPSec protocols and other protocols and products, have a birthday bound of approximately four billion blocks, which makes it easier for remote attackers to obtain cleartext data via a birthday attack against a long-duration encrypted session, as demonstrated by an HTTPS session using Triple DES in CBC mode, aka a "Sweet32" attack.	7.5 HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N
CVE-2015-4000	The TLS protocol 1.2 and earlier, when a DHE_EXPORT ciphersuite is enabled on a server but not on a client, does not properly convey a DHE_EXPORT choice, which allows man-in-the-middle attackers to conduct cipher-downgrade attacks by rewriting a ClientHello with DHE replaced by DHE_EXPORT and then rewriting a ServerHello with DHE_EXPORT replaced by DHE, aka the "Logjam" issue.	3.7 LOW	CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N
CVE-1999-0524	ICMP information such as (1) netmask and (2) timestamp is allowed from arbitrary hosts.	2.1 LOW	AV:L/AC:L/Au:N/C:P/I:N/A:N

CVE-2021-35237	A missing HTTP header (X-Frame-Options) in Kiwi Syslog Server has left customers vulnerable to click jacking. Clickjacking is an attack that occurs when an attacker uses a transparent iframe in a window to trick a user into clicking on an actionable item, such as a button or link, to another server in which they have an identical webpage. The attacker essentially hijacks the user activity intended for the original server and sends them to the other server. This is an attack on both the user and the server.	4.3 MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N
CVE-2019-14840	A flaw was found in the RHDM, where sensitive HTML form fields like Password has auto-complete enabled which may lead to leak of credentials.	7.5 HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N
CVE-2023-49255	The router console is accessible without authentication at "data" field, and while a user needs to be logged in in order to modify the configuration, the session state is shared. If any other user is currently logged in, the anonymous user can execute commands in the context of the authenticated one. If the logged in user has administrative privileges, it is possible to use webadmin service configuration commands to create a new admin user with a chosen password.	9.8 CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
CVE-2023-49262	The authentication mechanism can be bypassed by overflowing the value of the Cookie "authentication" field, provided there is an active user session.	9.8 CRITICAL	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
CVE-2023-49261	The "tokenKey" value used in user authorization is visible in the HTML source of the login page.	7.5 HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N
CVE-2023-49260	An XSS attack can be performed by changing the MOTD banner and pointing the victim to the "terminal_tool.cgi" path. It can be used together with the vulnerability CVE-2023-49255.	6.1 MEDIUM	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N
CVE-2023-49259	The authentication cookies are generated using an algorithm based on the username, hardcoded secret and the up-time, and can be guessed in a reasonable time.	7.5 HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N
CVE-2023-49257	An authenticated user is able to upload an arbitrary CGI-compatible file using the certificate upload utility and execute it with the root user privileges.	8.8 HIGH	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

CVE-2023-49256	It is possible to download the configuration backup without authorization and decrypt included passwords using hardcoded static key.	7.5 HIGH	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N
CVE-2023-49254	This CVE record has been updated after NVD enrichment efforts were completed. Enrichment data supplied by the NVD may require amendment due to these changes.	8.8 HIGH	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Affected Versions

Hongdian Router version V7.2.3_SE a and prior.

Mitigation

Upgrade to version V7.2.5_SE.

Support

If you have any questions about this security advisory, contact Hongdian Support Team.