Firmware for SDS-3000 and SDS-G3000 Series Release Notes

Version: v3.3	Build: 26072313
Release Date: Jul 31, 2026	

Applicable Products

SDS-3006, SDS-3006-2GTXSFP, SDS-3006-2GTXSFP-T, SDS-3006-4PoE-2GTXSFP, SDS-3006-4PoE-2GTXSFP-T, SDS-3006-T, SDS-3008, SDS-3008-T, SDS-3010-2GTXSFP, SDS-3010-2GTXSFP-T, SDS-3010-8PoE-2GTXSFP, SDS-3010-8PoE-2GTXSFP-T, SDS-3016, SDS-3016-2GSFP, SDS-3016-2GSFP-T, SDS-3016-2GTX, SDS-3016-2GTX-T, SDS-3016-T, SDS-G3006, SDS-G3006-2GTXSFP, SDS-G3006-2GTXSFP-T, SDS-G3006-4PoE-2GTXSFP, SDS-G3006-4PoE-2GTXSFP-T, SDS-G3006-T, SDS-G3008, SDS-G3008-T, SDS-G3010-2GTXSFP, SDS-G3010-2GTXSFP-T, SDS-G3010-8PoE-2GTXSFP, SDS-G3010-8PoE-2GTXSFP-T, SDS-G3016, SDS-G3016-2GSFP, SDS-G3016-2GSFP-T, SDS-G3016-T

Supported Operating Systems

N/A

New Features

• Adds support for VLAN Unaware mode.

Enhancements

• Adds additional configuration options for Domain UUID: Default / PROFINET / User-defined
• Users can now input a domain name in the SNMP Trap server URL.
• The device can now synchronize the system time when the DNS is not online during configuration.
• Adds support for importing SSL certificates.
• Adds support for additional MIB libraries.
• Upgrades jQuery to the latest version to prevent XSS attacks via the Management Interface and System Information pages.
• Upgrades GSDML to v2.44.
• Adds support for additional redundancy protocols in the TIA Portal topology view.
• Adds additional information to PROFINET-related event logs.

Bugs Fixed

• Users cannot retrieve MRP information through TIA Portal.
• The SNMP icon remains highlighted when SNMP is disabled.
• When refreshing the Bandwidth Utilization widget during any packet activity, the widget will show an initial value of 100% before gradually dropping off.
• Configuration files cannot be imported if an SFP-1FESLC transceiver module is installed.
• [CVE-2015-9251] jQuery versions prior to v3.0.0 may be vulnerable to Cross-site Scripting attacks, passing HTML from untrusted sources.
• [CVE-2019-11358] jQuery versions prior to v3.4.0 mishandle jQuery.extend because of Object.prototype pollution.
• [CVE-2020-11022] [CVE-2020-11023] jQuery versions later than v1.2 and prior to v3.5.0 may execute untrusted code when passing HTML from untrusted sources.
• [CVE-2020-23064] Cross Site Scripting vulnerability in jQuery v.2.2.0 until v.3.5.0 allows a remote attacker to execute arbitrary code via the <options> element.
• [CVE-2022-41311] [CVE-2022-41312] [CVE-2022-41313] Improper neutralization of input during web page generation.
• TIA Portal does not show an error indication on the SDS-3008 device icon if the shown physical connection is incorrect.

• PROFINET PLCs will show an error when connected to SDS-3000 devices via MRP.
• [CVE-2024-7695] An out-of-bounds write vulnerability caused by insufficient input validation allows attackers to overwrite memory beyond the buffer' s bounds.
• [CVE-2024-9137] Attackers could execute specified commands to perform unauthorized downloads or uploads of configuration files and system compromise.
• Rebooting the device when there is EtherNet/IP traffic causes a reboot loop.
• The switch name is deleted after a power cycle when the switch is in PROFINET mode.
• If the PN device name character limit is set to 240 and a PLC connection is being established while performing a firmware upgrade, the device may perform a cold start.
• When updating firmware from v2.2 to v3.2, the management VLAN will revert to its default settings.
• CVE-2011-1473 vulnerability issue. For more details, search the Security Advisories section on the Moxa website for the following Security Advisory ID: MPSA-262810.
• The system incorrectly generates specific PoE-related event logs when the event has not occurred. In rare cases, these false events may also disable PoE functionality.
• Users are unable to access the web console via port forwarding.

Changes

• SNMP is now enabled when PROFINET is actived.
• The device name and PROFINET device name are now unbound.
• When Mechatrolink is turned off, LLDP is automatically re-enabled.
• Removes a previously applied year 2038 limitation fix for compatibility reasons.

Notes

• This version removes a previously applied year 2038 limitation fix for compatibility reasons.

Version: v3.2	Build: 25042315
Release Date: May 23, 2025	

Applicable Products

N/A

Supported Operating Systems

N/A

New Features

• Added the MECHATROLINK-4 configuration option to the web interface and DIP switch.

Enhancements

• Added support for the standard MRP MIB library.

Bugs Fixed

• [CVE-2025-1680] An open redirect vulnerability occurs when an application allows a user to control a redirect or forward to another URL.

Changes

N/A

Notes

• Upgrading firmware from v2.2 or earlier to v3.0 or later will reset the management VLAN to its default value (VLAN 1). Other VLAN settings are not affected. If you upgraded the firmware under the aforementioned conditions, please use VLAN 1 to access the switch and reconfigure the relevant settings. Contact your local Moxa Technical Support team if you need further assistance.

Version: v3.1	Build: 25022018
Release Date: Mar 18, 2025	

Applicable Products

N/A

Supported Operating Systems

N/A

New Features

N/A

Enhancements

N/A

Bugs Fixed

• [CVE-2024-7695] An out-of-bounds write vulnerability caused by insufficient input validation allows attackers to overwrite memory beyond the buffer's bounds.
• [CVE-2024-9404] Due to insufficient input validation, exploitation of the moxa_cmd service could lead to denial-of-service or service crashes.
• [CVE-2024-9137] Attackers could execute specified commands to perform unauthorized downloads or uploads of configuration files and compromise the system.
• [CVE-2024-12297] Frontend authorization logic disclosure vulnerability.
• After rebooting the switch, the system name is deleted in PROFINET applications.
• The switch cannot be accessed through the management VLAN with certain VLAN configurations.

Changes

N/A

Notes

• Upgrading firmware from v2.2 or earlier to v3.0 or later will reset the management VLAN to its default value (VLAN 1). Other VLAN settings are not affected. If you upgraded the firmware under the aforementioned conditions, please use VLAN 1 to access the switch and reconfigure the relevant settings. Contact your local Moxa Technical Support team if you need further assistance.

Version: v3.0	Build: 24070920
Release Date: Sep 30, 2024	

Applicable Products

SDS-3006 Series, SDS-3008 Series, SDS-3010 Series, SDS-3016 Series, SDS-G3006 Series, SDS-G3008 Series, SDS-G3010 Series, SDS-G3016 Series

Supported Operating Systems

N/A

New Features

• Added support for the Trusted Access function.
• Added support for the Fiber Check function.
• Added support for Smart PoE features.

Enhancements

• For security reasons, the Modbus/TCP protocol is now disabled by default.
• Supports TLS v1.3.

Bugs Fixed

• [CVE-2015-9251] jQuery versions prior to v3.0.0 may be vulnerable to Cross-site Scripting attacks.
• [CVE-2019-11358] jQuery versions prior to v3.4.0 mishandle jQuery.extend because of Object.prototype pollution.
• [CVE-2020-11022] [CVE-2020-11023] jQuery versions later than v1.2 and prior to v3.5.0 may execute untrusted code when passing HTML from untrusted sources.

Changes

N/A

Notes

• Upgrading firmware from v2.2 or earlier to v3.0 or later will reset the management VLAN to its default value (VLAN 1). Other VLAN settings are not affected. If you upgraded the firmware under the aforementioned conditions, please use VLAN 1 to access the switch and reconfigure the relevant settings. Contact your local Moxa Technical Support team if you need further assistance.

Version: v2.2	Build: N/A
Release Date: Sep 08, 2023	

Applicable Products

SDS-3008 Series, SDS-3016 Series

Supported Operating Systems

N/A

New Features

• Added support for the MRP Manager function.

Enhancements

• The SNMP protocol is now disabled by default to improve security.

Bugs Fixed

• Users are unable to enable or disable ports through EtherNet IP.
• The MRP status cannot be displayed after importing a GSD file.
• Importing a GSD file will show an error in the TIA portal.
• [CVE-2022-40691] A specially crafted HTTP request can lead to disclosure of sensitive information.
• [CVE-2022-40224] A specially-crafted HTTP message header can lead to denial of service.

Changes

• Removed the recommended browser notice from the web interface.

Notes

N/A

Version: v2.1	Build: FWR_SDS3000_V2.1_Build_21042817.
Release Date: May 06, 2021	

Applicable Products

SDS-3016 Series, SDS-3008 Series

Supported Operating Systems

N/A

New Features

• Adds support for MXview v3.2.

Enhancements

N/A

Bugs Fixed

N/A

Changes

N/A

Notes

N/A

Version: v2.0	Build: N/A
Release Date: Mar 31, 2021	

Applicable Products

SDS-3016 Series, SDS-3008 Series

Supported Operating Systems

N/A

New Features

• Add SDS-3016 Series.
• Web-based GUI for port diagnostics with statistics to detect and prevent issues.
• Supports MRP client redundancy based on IEC 62439-2 to ensure high network availability.
• IP port binding to ensure critical devices can be replaced quickly without reassigning the IP Address.
• Add QoS/DSCP for data priority.
• Static port lock to enhance network security.

Enhancements

N/A

Bugs Fixed

N/A

Changes

N/A

Notes

N/A

Version: v1.2	Build: FWR_SDS3008_V1.2_Build_20012019
Release Date: Jan 31, 2020	

Applicable Products

SDS-3008 Series

Supported Operating Systems

N/A

New Features

N/A

Enhancements

• [MSRV-2017-011][CVE-2019-6561] Supports browser cookie parameters “same-site” to eliminate CSRF attacks.

Bugs Fixed

• Login issue with Chrome v65.
• The system rebooted when SNMP GET with request ID=0.
• Log in issue after a new user was created in the multi-language webpage.
• [MSRV-2017-006][CVE-2019-6557] Buffer overflow vulnerabilities that may have allowed remote control.
• [MSRV-2017-007][CVE-2019-6522] An attacker could read device memory on arbitrary addresses.
• [MSRV-2017-009][CVE-2019-6565] No proper validation of user inputs, which allows users to perform XSS attacks.
• [MSRV-2017-011][CVE-2019-6561] CSRF attacks were possible if browser cookie parameters were not correct.
• [MSRV-2017-012][CWE-121] A stack-based buffer overflow condition whereby the buffer that was being overwritten was allocated on the stack.

Changes

N/A

Notes

• MSRV is Moxa's internal security vulnerability tracking ID.

Version: v1.1	Build: Build_17060809
Release Date: Aug 03, 2017	

Applicable Products

SDS-3008, SDS-3008-T

Supported Operating Systems

N/A

New Features

• Multi-language web GUI: English, Traditional Chinese, Simplified Chinese, Japanese, German, and French.

Enhancements

• Optimize web page loading performance.

Bugs Fixed

N/A

Changes

N/A

Notes

N/A

Version: v1.0	Build: Build_16122620
Release Date: N/A	

Applicable Products

SDS-3008, SDS-3008-T

Supported Operating Systems

N/A

New Features

• First release.

Enhancements

N/A

Bugs Fixed

N/A

Changes

N/A

Notes

N/A