SmartCS NS-2250 Console Server

Release Notes

Version 2.2

Seiko Solutions Inc.

Table of contents

Version 2.2 (2020/10/30)

Version 2.2 provides following new features and updates.

1 Add SNMP Version 3 function

SNMP Version 3 has been supported for the Get request from SNMP server and Trap transfer.
Contents of MIB and Trap are same as Version 1 and Version 2(2c).

Specifications of SNMP Version 3 are as follows.

Item	Detail
Authentication algorithm	HMAC-MD5-96 / HMAC-SHA-96
Encryption algorithm	DES-CBC / AES128-CFB

Following commands have been added or expanded because of adding this function.

Command	Detail
set snmp engineid	Configure the snmpEngineID notified in SNMP Version 3.
set snmpuser name	Configure the user, authentication algorithm and encryption algorithm used in SNMP Version 3.
set trap manager	Configure the SNMP server and version to send SNMP trap. “Version 3” can be specified as SNMP version.

2 Expand supported IPv6 function

The functions available in IPv6 communication have been expanded.
The functions corresponding to IPv6 depend on system software version as follows.

Category	Function	v1.3 and above	v2.2 and above
Port access	Port server	○	○
	Port log sending(SYSLOG/NFS/FTP/Mail)	-	○
Management	DNS client	○	○
	Static routing	○	○
	Telnet/SSH server	○	○
	Telnet client	○	○
	FTP/SFTP server	FTP - / SFTP ○	FTP ○ / SFTP ○

	Bonding	○	○
	SNTP client	-	○
	SNMP agent	-	○
	SYSLOG client	-	○
	FTP/TFTP client	-	○
Security	Access control(allowhost)	○	○
	RADIUS authentication/accounting	-	○
	TACACS+	-	○
	Firewall(ipfilter)	-	○
	IPsec	-	-

3 Fix bug related to SNMP response

The bug that NS-2250 sends wrong response to SNMP get request for “IF-MIB ifLastChange” has been fixed.
NS-2250 does not support “IF-MIB ifLastChange” and always returns “0” regardless of the type of interfaces.

Version 2.1 (2019/10/18)

Version 2.1 provides following new features and updates.

1 Supporting SSH transparent connection (sshxpt)

SSH transparent connection (sshxpt) has been added to the port server function, enabling transparent communication with target devices by specifying the TCP port number assigned to each serial port of NS-2250. It also enables to operate third-party Ansible modules to work via NS-2250

Specifications of SSH transparent connect function are as follows.

Item	Detail
Activation	The sshxpt option in the set portd tty session command activates the TCP port for sshxpt on the specified serial port.
User	To use this function, it requires creating new users in portusr group and configuring the serial ports accessible to the user.
TCP port	Starting TCP port number can be changed by “set portd sshxpt” command. The default port number starts from 9301 and the consecutive port numbers are assigned to each serial port.
Protocol	This function has to be used via SSH and it is unable to connect via Telnet or Console.
Operation when starting the connection	Line feed code specified by “set portd tty connted send_nl” command is sent when starting the sshxpt connection.

2 Expand exclusion between portd normal session and tty manage function

Exclusion between portd normal session and tty manage function can be disabled by “set portd service exclusive” command.
When the exclusive function is enabled (default setting), users can not access target devices when a session of portd normal (rw session) or tty manage function already exists.
When the exclusive function is disabled, there is no exclusion for each session.
Verification gets easier because of this function.

3 Expand tty manage function

- "show log ttymanage send" command
Users can confirm the commands which are sent to target devices using tty manage function.

- Control character sending function
Users can send control characters using tty manage function.
33 kinds of control characters from "Ctrl-@" (0x00) to "Ctrl-_" (0x1f), and "DELETE" (0x7f) are available.

4 Change identification character of SSH protocol version

Identification character of SSH protocol version has been changed to "SSH-2.0-port_sshd".

5 Fix bug related to listen port

The bug that makes TCP port for direct mode session opened has been fixed.
This bug occurs when the specific commands are executed after "set portd tty session" command with select mode.

6 Fix bug tty manage function

The bug that control characters and subsequent commands might not be sent to target devices when specifying control characters in "input" option using tty manage function has been fixed.

7 Respond to Linux Kernel (TCP SACK PANIC) vulnerability

Following vulnerabilities have been addressed.

CVE-2019-11477
The vulnerability that modified SACK sequences may cause an integer overflow and Kernel Panic.

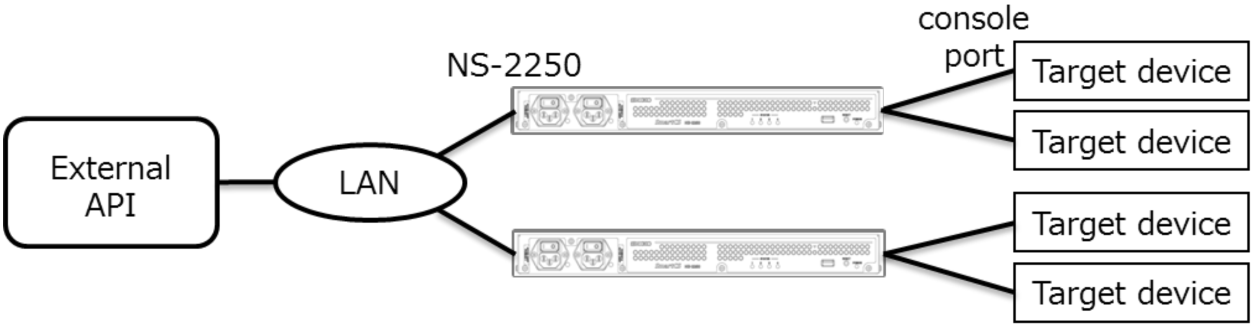
CVE-2019-11478
The vulnerability that modified SACK sequences may cause a fragment to TCP retransmission queue.

Version 2.0 (2019/4/12)

Version 2.0 provides following new features and updates.

1 Supporting tty manage function

tty manage function has been added that allows to change the settings and obtain information of target devices connected to the serial ports of NS-2250. This function enables to operate the target devices using external API or orchestration tool.
Creating new users in extusr group and enabling tty manage function is required before using this function.



Specifications of tty manage function are as follows.

Item	Detail
User	To use this function, it requires creating new users in extusr group and granting tty manage permission. If you do not have tty manage privileges, you will have the same privileges as a user in the normal group. When executing commands such as “ttysend” and “ttylog”, you must configure the serial ports accessible to the user. Up to 10 users in extusr group can be registered. (UID: 401-410)
Activation	This function will be enabled by “enable ttymanage” command.
Protocol	This function has to be used via SSH and it is unable to connect via Telnet or Console.
Command	Following operations can be executed after logging in as auser in extusr group. “ttysend” command: sending and receiving characters “ttylog” command: displaying and deleting port logs
Access to target devices	Only one command, such as ttysend, can be executed at a time on

	one serial port of NS-2250.
Exclusion with portd normal session	Users can not access target devices using tty manage function when portd normal sessions (rw session) already exist and vice versa. Users can not access target devices using portd normal sessions when the session of tty manage function exists. portd monitor sessions (ro session) are exceptional for this exclusion.

2 Add new commands and option parameters

- An option parameter of "disconnect" command

Users can disconnect the sessions of normal user, extusr and root user by specifying terminal device number as an option parameter of "disconnect" command after confirming the terminal device number with "show user login" command.

- An option parameter of "show interface" command

Users can confirm the individual interface information of NS-2250 by specifying the interface as an option parameter of "show interface" command.

In addition to the above commands, new commands and option parameters have been added and the output of some commands has been changed in accordance with the addition of the tty manage function.

3 Add error message when detecting RTC abnormality

The error message is output to the console logs when RTC error is detected.

4 Fix bug related to the port number of Mail server

The bug that caused the port number of Mail server not being deleted when the Mail server setting registered as the destination of the port logs was deleted has been fixed.

5 Respond to DoS vulnerability due to resource depletion

Following vulnerability has been addressed.

CVE-2018-5391
The vulnerability that a denial of service condition may be caused by receiving specially crafted IP fragments is modified.

Version 1.3 (2017/4/14)

Version 1.3 provides the following new features and fixes.

1 Support for IPv6

In this version, IPv6 is added to run the NS-2250 in the IPv6 network.
It supports IPv4/IPv6 dual stack. The functions corresponding to IPv6 are followings.

Category	Function	State
Port access	Port server	○
	Port log sending(SYSLOG/NFS/FTP/Mail)	-
Management	DNS client	○
	Static routing	○
	Telnet/SSH server	○
	Telnet client	○
	FTP/SFTP server	FTP - / SFTP ○
	Bonding	○
	SNTP client	-
	SNMP agent	-
	SYSLOG client	-
	FTP/TFTP client	-
Security	Access control(allowhost)	○
	RADIUS authentication/accounting	-
	TACACS+	-
	Firewall(ipfilter)	-
	IPsec	-

The default value of IPv6 is “disable”, and IPv6 address is not set.
After enable IPv6 by the “create ip6” command, set IPv6 address by the “set ip6addr” command.

2 Change the operating specification when accessing the port server by telnet

In the case of using in the select mode, even if being set to deny the telnet access by not specifying “telnetd/portd telrw/portd telro” in the “create allowhost” command the port select menu is displayed but change the operating specification not to be displayed.

3 Change the specification of sending the mail

Change the specification to insert the DATE/FROM data in the SMTP header when sending the port log by mail.

4 Change the specification of the “traceroute” command

When the DNS server is set in the setting of the NS-2250 the IP address in the output result of the “traceroute” command is displayed to convert to the hostname, but change the specification to be displayed in the form of the IP address.
If there is no response from the DNS server the “traceroute” command becomes not to be kept waiting until the timeout elapsing.

5 Fix for the DoS vulnerability

Fix the following vulnerabilities.

CVE-2017-5970
The vulnerability that the kernel may crash because of receiving the packet whose IP option is modified.

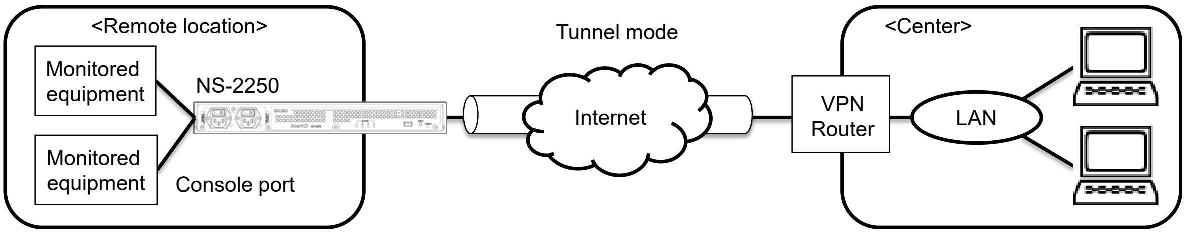
CVE-2017-6214
The vulnerability that an infinite loop may occur because of receiving the TCP packet in which the URG flag is set.

Version 1.2 (2016/10/28)

Version 1.2 provides the following new features and fixes.

1 Support for IPsec encryption

This version added IPsec to encrypt between the NS-2250 and VPN routers. The connection mode supports to both IPsec Initiator and Responder. It supports cryptographic key authentication with pre-shared key (PSK), and the maximum number of connections is 8.



The below table shows the connection mode and the operation mode as well as the number of the available connections.

Item	Description
Connection mode	Cryptographic key authentication by the pre-shared key (PSK)
Operation mode	Tunnel mode
The number of the available connections	Max. 8 connections. The configuration to establish the IPsec connection by the opposite network (subnet) is required.
Monitoring	Detect disconnection of tunnel interface by DPD
Others	NAT traversal (UDP capsuling for ESP)

NS-2250 supports the following IKE ISAKMP-SA (Phase1).

Item	Description
IKE protocol	IKEv1/IKEv2
Encryption algorithm	3DES/AES128/AES128CTR/AES256
Authentication algorithm	MD5/SHA1
DH group	2(1024bit)/5(1536bit)/14(2048bit)
ISAKMP-SA life time	3600～86400 sec. (Default: 10800 sec.)

NS-2250 supports the following IPsec-SA (Phase2)

Item	Description
Encryption algorithm	3DES/AES128/AES128CTR/AES256
Authentication algorithm	HMAC-MD5/HMAC-SHA1
DH group (during PFS)	2(1024bit)/5(1536bit)/14(2048bit)
IPsec-SA life time	3600～86400sec. (Default: 3600 sec.)

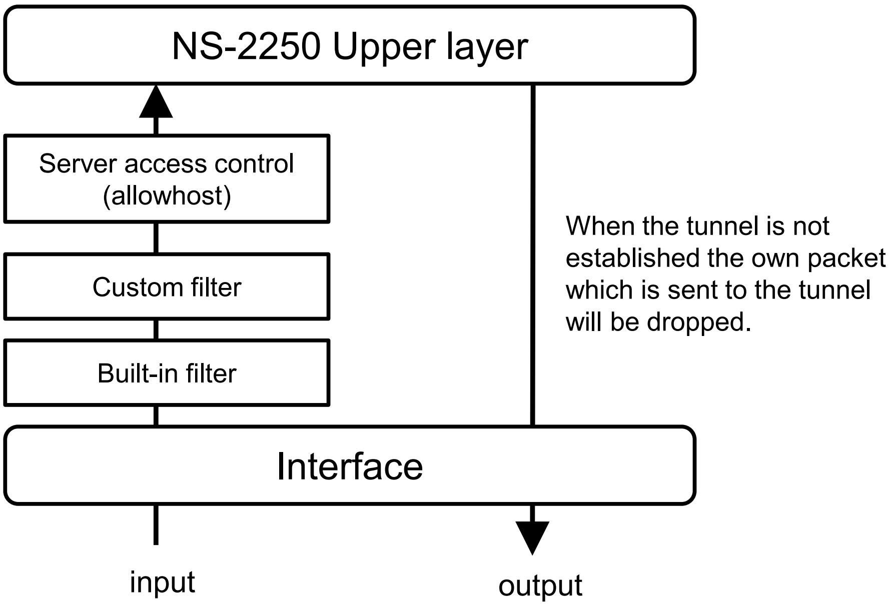
2 Support for Firewall (ipfilter)

Firewall (ipfilter) has been added to enhance security. It supports built-in filters and custom filters on the receiving interface. With the Firewall you can achieve the access control by respective filter conditions such as IP address, protocol type and port number.
The maximum number of registrations is 64 entries for the NS-2250.

Item		Description
Filter Type	Built-infilter (receive)	The built-in filter is a filter which is configured in the system in advance. It accepts the following received packets. (1) Return packet for packet sent by NS-2250 The following packets are also subject to this filter. ・SYN/ACK and ACK packet at 3-way handshake ・FIN, FIN+ACK and RST packet at end of session ・TCP connection request packet (SYN) of FTP-DATA session (passive) when accessing ftpd function ・TCP connection request packet (SYN) of FTP-DATA session (active) when ftp command is executed ・IKE packet after establishing ISAKMP-SA ・ESP packet after establishing IPSEC-SA ・ICMP error message packet (2) Packet sent out from loopback device of NS-2250 Triggered by enabling the Firewall. (Default: disable) Deleting or modifying the built-in filter is not possible.
	Custom filter (receive)	User configurable filter processed at the input of the interface. Processed after the built-in filter. Max. 64 entries can be stored.

Filter condition	Interface	eth1: LAN1 port eth2: LAN2 port bond1: Bonding port
	IP address	SA: Source IP address DA: Destination IP address
	Protocol	ICMP: ICMP type(0-255) TCP: TCP port number(1-65535) UDP: UDP port number(1-65535) ESP: ESP protocol
	Processing	accept: accept the packet drop: drop the packet

When Firewall (ipfilter) become enabled each filter will be evaluated in the order shown below.


NS-2250 Upper layer
Server access control (allowhost)
Custom filter
Built-in filter
When the tunnel is not established the own packet which is sent to the tunnel will be dropped.
Interface
input
output

3 Enhancement for escape character of Telnet client

In previous version, the escape character of Telnet client was fixed to Ctrl +]. In this version, you can change and disable the escape character. Even if you use Telnet login via jump server many times, you will be able to perform operations such as disconnecting Telnet sessions. This function can be used with "set telnet cmdchar" command.

4 Support for function to change Interface MTU

The function to change the Interface MTU was added. This function can be used with "set ipinterface mtu" command.

5 Fix for Off-Path TCP Exploits vulnerability (CVE-2016-5696)

The TCP protocol is implemented according to RFC 5961 to limit the amount of Challenge ACK transmission in preparation for DOS attacks. This version responded to vulnerabilities that may be subject to attacks of connection disconnection and data injection using the restriction.