STORMSHIELD ENDPOINT SECURITY EVOLUTION

RELEASE NOTES

Version 2

Document last update: December 17, 2020

Reference: ses-en-release_notes-v2.0.1

Table of contents

In the documentation, Stormshield Endpoint Security Evolution is referred to in its short form: SES Evolution.

This document is not exhaustive and minor changes may have been included in this version.

Resolved vulnerabilities for SES Evolution 2.0.1

Protection against denial of service attacks added
Protection against DDoS attacks was added to the API that registers new agent handlers in the Backend. Now only one agent handler can be registered every 15 seconds.

Value in the registry deleted
A value relating to the security of challenges was unnecessarily present in the registry. This vulnerability was fixed by deleting this value.

SES Evolution 2.0.1 fixes

Installing SES Evolution

Password fields
In the Installation Center, the password and confirm password fields are now always correctly verified.

License validity
In the Installation Center, the format and validity of the license are verified as soon as the license file is selected, instead of at the end of the installation.

Security Policies

Support reference: 177214CW

Network access
Some types of network access were not filtered by application protections because they were initiated by the system. They can now be blocked. This option makes it possible to block remote access to shared folders located on workstations that are protected by the SES Evolution agent.

If you upgrade SES Evolution to version 2.0.1, the default policy is not updated. You can download the corresponding rule set from your MyStormshield personal area to add network access rules for system process. For more information, refer to the Stormshield Knowledge Base.

Network IDs
The **Invert identifier scope** option is now correctly saved in the network ID editing window.

Audit rules on drivers
Specific behavior in the *Driver loading* and *Driver integrity* protection rules is now correctly applied. These rules no longer generate unjustified logs for allowed drivers.

Logs

Searching in agent logs

In the administration console, the maximum duration of an agent log search has been increased from 30 seconds to 15 minutes. A message now appears when the search exceeds this duration.

Displaying incidents

When an incident is opened in the Agent Logs panel, only alert logs are now displayed, up to a maximum of 1000 logs. The remaining logs are loaded when the attack chart is consulted, up to a maximum of 100000 logs. This makes it possible to build an attack chart with comprehensive logs.

SES Evolution Agent

Deploying policies

Lengthy logs no longer cause the graphical interface of the SES Evolution agent to unexpectedly shut down.

Self-protection rules

Self-protection rules on some registry keys of SES Evolution agents were not correctly applied. This issue has been fixed.

Display

Windows 10 agents

The **Agents** panel in the administration console now displays the correct version of the operating system for Windows 10 agents.

Compatible Microsoft Windows versions

SES Evolution 2 is compatible with the following Windows versions. For more information, see section System requirements for SES Evolution of the *Installation guide*.

Administration console
Windows 7 in 32 and 64 bits
Windows 8.1 update - August 2014 - 32/64 bits
Windows 10 Enterprise 2015 LTSB - 32/64 bits Windows 10 Enterprise 2016 LTSB - 32/64 bits Windows 10 1809 - 32/64 bits Windows 10 1909 - 32/64 bits Windows 10 2004 - 32/64 bits
Windows Server 2008 R2
Windows Server 2012 R2 *
Windows Server 2016
Windows Server 2019

Backend
Windows Server 2012 R2 *
Windows Server 2016
Windows Server 2019

Agent handler
Windows 10 Enterprise 2015 LTSB – 64 bits Windows 10 Enterprise 2016 LTSB – 64 bits Windows 10 1809 – 64 bits Windows 10 1909 – 64 bits Windows 10 2004 – 64 bits
Windows Server 2008 R2*
Windows Server 2012 R2*
Windows Server 2016
Windows Server 2019

* On these newly installed operating systems, Framework .NET 4.6.2 must be installed beforehand to enable the SES Evolution Installation center to run.

Agent
Windows 7 in 32 and 64 bits
Windows 8.1 update 3 (August 2014) - 32 or 64 bits
Windows 10 Enterprise 2015 LTSB - 32/64 bits Windows 10 Enterprise 2016 LTSB - 32/64 bits Windows 10 1809 - 32/64 bits Windows 10 1909 - 32/64 bits Windows 10 2004 - 32/64 bits Windows 10 20H2 – 32 et 64 bits
Windows Server 2008 R2
Windows Server 2012 R2
Windows Server 2016
Windows Server 2019

Known issues

The up-to-date list of the known issues related to this version of SES Evolution is available on the Knowledge Base Stormshield (English only). To connect to the Knowledge base, use the same identifiers as for MyStormshield.

Explanations on usage

Bluetooth Low Energy devices
The SES Evolution agent does not filter Bluetooth Low Energy devices; only standard Bluetooth devices are recognized.

Compatibility with other firewalls
In some cases, when another firewall with a priority higher than the SES Evolution agent's priority is installed on the same workstation and pauses the processing of a packet, regardless of its decision on how to process the packet, SES Evolution will never analyze it.

Documentation resources

The following technical documentation resources are available on the Stormshield Technical Documentation website or on Stormshield Institute website. We suggest that you rely on these resources for a better application of all features in this version.

Guides

- Installation guide
- Administration guide

Previous versions of SES Evolution v2

In this section, you will find the features and fixes from previous versions of SES Evolution v2.

2.0.0	New features

Summary of the features

The version 2.0 of SES Evolution provides the following features.

SES Evolution 2.0 features

Protection	
Memory overflow	Protects your pool from intrusion attempts and vulnerability exploitation.
Process hollowing	
Security token theft	
File system bypass	
Keylogging	
File access control	Controls all system resources and access to them. Allows applications to make changes, access these resources or blocks them. You can also simply monitor them.
Registry base access control	
Memory access control	
Execution control	
Driver loading detection	Detects rootkits that attempt to load or change drivers in the kernel.
Driver alteration detection	
Application firewall	Controls incoming and outgoing network communications for each application.
Wi-Fi access point control	Manages allowed Wi-Fi networks and prevents the Wi-Fi-LAN bridge from being set up.
Floppy disk or CD/DVD drive control, serial ports	Controls devices allowed in your pool through fully customizable rules.
Bluetooth device control	
USB device control	
USB decontamination air gap	Controls the USB keys and hard disks in your pool, manages trusted devices and blocks devices that have not been validated.

Configuration	
Management via agent groups	Organizes your pool according to your requirements through a simple but powerful system of agent groups.
Configuration deployment	Deploys new configurations in all agents with a single click in the administration console.
Stormshield security policy	Protects your pool with a default policy that covers common threats and adds custom security rules to fully adapt the policy to your environment.
Context-based security policies	Adapts security to agents' environment so that they apply different policies based on their location.
Policy management through rule sets	Pool security rules in your policies and manage exceptions easily.

Scheduled tasks	Runs commands on agents by configuring scripts from the administration console.
Agent modularity	Manages features installed on each agent from the administration console: uninstall unused features, delete incompatible versions and reduce the attack surface.
Challenges	Allows some operations to be performed securely through a question/response system.
Simultaneously connected administrators	Organizes your administrators by role to manage simultaneous access to various resources on the administration console.

Activity monitoring	
Dashboard	See the status of your pool in a glimpse with a simple dashboard.
Log tracking	Views events that agents raise, filtering them by priority, type, group, etc.
Attack analysis	Follows incidents and analyzes attacks in a dedicated panel that illustrates steps in charts and provides additional information to better understand each attack.
Agent monitoring	Tracks the pool's agents in real time, checks their status and assigns them to groups
Syslog server export	Exports all events in your SIEM system to include them in your other sources of security information (firewall, antivirus, etc.).

Contact

To contact our Stormshield Technical Assistance Center (TAC):

- https://mystormshield.eu/
  All requests to technical support must be submitted through the incident manager in the private-access area https://mystormshield.eu, under Technical support > Manage cases.
- +33 (0) 9 69 329 129
  In order for us to provide high-quality service, you are advised to use this communication method only to follow up on incidents that have been created earlier on https://mystormshield.eu.

STORMSHIELD