STAIRWELL

Stairwell Windows Forwarder 1.6.0 Release Notes

Version: 1.6.0.0
Date: Jun 18, 2024

New Features

- Enhanced diagnostic abilities for quicker troubleshooting in the field. This includes:
  - Kernel logging (FOR-209, FOR-216, FOR-243, FOR-244)
  - Kernel counters (FOR-210)
  - Crash dump collection when the service encounters a fatal error (FOR-212)
  - New strategy for versioning, to make it easy to catch mismatched binaries in the field (FOR-236)
  - The installer now supports the LOGLEVEL parameter, to obtain logging as soon as the service starts. Supported values range from 0 (all log messages) through 5 (fatal log messages only). The default is 2 (informational log messages) (FOR-233)
  - Collection of diagnostics (FOR-214)
- Improved performance during module load processing (FOR-237)

Bug Fixes

- Fixed cases where sightings were missed for files extracted from archives (FOR-257)
- In cases where the forwarder service crashes, restart it automatically (FOR-211)
- Fixed a rare BSOD seen just after the driver loaded, or just before it unloaded (FOR-218, FOR-239)
- Fixed cases where sightings of the EICAR file were missed, due to the file extension (FOR-233)
- Ensured kernel memory is zeroed out on all supported platforms (FOR-245)
- Updated the maximum file size limit to 512MB due to bandwidth considerations. (FOR-252)
- Renamed kernel pooltags to avoid collisions with existing Microsoft pooltags. This was not a functional issue but prevented reliable analysis of memory-related issues (FOR-246)
- Improved security on the local communication port, used between the service and the driver (FOR-242)
- Added protocol version to service / driver communication, to prevent potential issues when mismatched (FOR-241)

STAIRWELL

- Fixed a bug where upgrades were reported as failed, even if they succeeded (FOR-198)

Known Issues

- We recommend installing to the default directory. If you install to a custom directory and upgrade, the upgraded version will be installed to the default directory (FOR-258)
- There is a known issue with Microsoft Filter Verifier that results in a BSOD when running against our driver. We recommend that you avoid enabling Driver Verifier on swagent.sys until we release a workaround. See the Microsoft documentation for more details. (FOR-277)

File Details

SHA256 Hash	File Name	File Version
F38EE825D29349C92F28C40879993A100A3F1FB00DFA1D8F2E1C86A05B43C2B6	StairwellForwarderBundle-1.6.0.0.exe	1.6.0
48514414F9071EDFE992171CE0E904F0162A17AAED6F72C247210B0DE52720F0	StairwellForwarder-1.6.0.0.exe	1.6.0
B941F5AC5F83197660A816AD7DD772F1BC7ABD0B3A7F618CBD12CC52196650AD	StairwellForwarderInternal-1.6.0.0.msi	1.6.0
6D13673067ACC8B6544CE561860927C7B6E91776439D08F1C8F5FAF8CE9B0FA3	SWAgent.sys	2.1.1
94756B839C91AF71669192DB0B3A23D02A179B0EB704F30DEE7B0D42A5C790C9	SwellService.exe	1.6.0
008EF55682ED5605901AB7F1B35E8F71BA7F31AAEAF4BAA20DE25B19793404A8	SWLib.dll	1.6.0