Release Notes

Revision B

McAfee Endpoint Security 10.7.0

April 2020 Update

For use with ePolicy Orchestrator

Contents

Rating

The rating defines the urgency for installing this update.

Rating – Mandatory

Mandatory	Critical	High Priority	Recommended

Mandatory

- Required for all environments.
- Failure to apply Mandatory updates might result in a security breach.
- Mandatory updates and hotfixes resolve vulnerabilities that might affect product functionality and compromise security.
- You must apply these updates to maintain a viable and supported product.

For more information, see KB51560.

What's new in the April 10.7.0 release

This update includes fixes and resolution for several issues, as well as cumulative fixes from the previous monthly updates.

Additional Information

Note: If Endpoint Security 10.7 April Update is installed on unpatched Microsoft Windows 7 or Server 2008 R2 for Microsoft KB4474419 then a notification prompt appears notifying that the installation is not SHA1 signed.

This will occur regardless of installation method used. This is because Microsoft has fully deprecated SHA1 signing in their switch from dual signing with SHA1/SHA2 to SHA2 only.

This does not affect Endpoint Security 10.7 April Update's ability to successfully install.

The pop-up will not be experienced on Windows 7 SP1or Server 2008 R2 SP1 and above. In order to avoid this scenario, McAfee recommends that you apply the necessary Windows patches.

This release includes the following build numbers:

Component	Version
Endpoint Security Platform	10.7.0.1675
Endpoint Security Platform extension	10.7.0.566
Endpoint Security Threat Prevention	10.7.0.1705
Endpoint Security Threat Prevention extension	10.7.0.585
Endpoint Security Firewall	10.7.0.1198
Endpoint Security Firewall extension	10.7.0.541
Endpoint Security Web Control	10.7.0.1473
Endpoint Security Web Control extension	10.7.0.550
Endpoint Security Adaptive Threat Protection	10.7.0.1886
Endpoint Security Adaptive Threat Protection extension	10.7.0.562
Threat Detection Reporting	1.0.0.371
Endpoint Security Migration Extension	10.7.0.275

For more details about the product versions listed in Control Panel, see KB92355.

Resolved issues in the April 10.7.0 release

This release resolves known issues from the previous releases of the product.

For a list of current known issues, see McAfee Endpoint Security 10.x Known Issues (KB82450).

Platform

Component	Reference	Resolution
Security	ENSW-27879	Vulnerability related to privilege escalation related to mctray.exe has been resolved - see CVE-2020-7274.
Security	ENSW-28309	Vulnerability related to potential compromise of uninstall binary paths has been resolved - see CVE-2020-7275.
Installation	ENSW-94600	Customer are now able to install Endpoint Security 10.7 using command line verbose logging options.
Installation	ENSW-96956	Fixes the issue where SCCM 1910 hangs on systems with ENS 10.6.1 or 10.7.0 installation.
Feature Fix	ENSW-97044	Resolved an issue where users with valid permissions were not able to make changes to common settings.
Security	ENSW-97682	Vulnerability related to Endpoint Security process protection is now resolved – see CVE-2020-7277.
Installation	ENSW-99067	Lotus Notes email scanner now uninstalls successfully when migrating from VSE to ENS.

Threat Prevention

Component	Reference	Resolution
Feature Fix	ENSW-25718	On-demand Scan schedule now starts successfully after upgrading to Endpoint Security.
Performance	ENSW-28267	Fixes an issue with the AMSI feature of On-access Scan that caused high-CPU usage by mcshield.exe on IIS cluster server.
Feature Fix	ENSW-28351	OAS ScriptScan Exclusions are being honored consistently.
Feature Fix	ENSW-28941	ODS with and without Scan cache option shows incorrect scan result.
Installation	ENSW-29251	Upgrade from 10.6.1 to 10.7 now properly retains custom scan configuration in standalone mode.
Feature Fix	ENSW-94601	Paths containing '/' when entered under 'Exclusion by detection name' are now accepted.
Performance	ENSW-96082	Resolved an issue causing audio distortion during content updates and property collection.
Feature Fix	ENSW-96184	Access protection rule '`Browsers booting files from the Downloaded Program Files folder`' now also blocks the execution for Microsoft Edge and Internet Explorer.

Feature Fix	ENSW-96512	Access Protection events with invalid dates are no longer sent to debug but are now parsed by ePO for audit purposes.
Installation	ENSW-96516	Resolved an install issue with the error “Database could not be opened”
Security	ENSW-96901	Using the access protection rule, user is now restricted to rename/delete programs in the autorun registry key - see CVE-2020-7273
Installation	ENSW-96918	Resolved an issue where an ENS Installation repair window would pop up when launching Windows Explorer.
Performance	ENSW-96652	Resolved an issue with slow logon related to load library.
Feature Fix	ENSW-97259	ENS Access Protection rule names are now restricted to 128 characters to allow parsing into ePO database.
Performance	ENSW-97679	Improved website access performance in Internet Explorer when Script Scan is enabled.
Feature Fix	ENSW-97712	Resolved issue where Internet Explorer 11 would fail to load pages in Citrix environments when Script Scan was enabled.
Feature Fix	ENSW-98053	Resolved an issue where weekly on demand scans were repeated daily when the “Run if missed” option was selected.

Adaptive Threat Protection

Component	Reference	Resolution
Feature Fix	ENSW-97190	Resolved an issue where McAfee Active Response was not functions properly after upgrading to ENS 10.6.1 December 2019 or ENS 10.6.1/10.7 February 2020.

Firewall

Component	Reference	Resolution
Feature Fix	ENSW-25783	Resolved an issue with Firewall adaptive rule aggregation.
Feature Fix	ENSW-28813	Resolved an issue with Firewall was blocking return traffic for an application.
Feature Fix	ENSW-29111	ENS firewall no longer blocks legitimate Windows 10 processes when the policy settings "Block all untrusted executables” and GTI “Block traffic” were enabled and GTI was unreachable.
Feature Fix	ENSW-29209	Wildcard ‘*’ is now allowed on Endpoint Security client if used instead of drive letter in Endpoint Security Firewall rule policy.
Feature Fix	ENSW-95914	Firewall options policy applied in McAfee ePO is now visible.
Feature Fix	ENSW-97019	Resolved an issue where GTI inappropriately blocked Microsoft PPTP client.
Feature Fix	ENSW-97491	Resolved an issue where a rule based on the SDN was not matched consistently.
Feature Fix	ENSW-97695	Resolved an issue where the network card initialization takes up to two minutes to launch following installation of Endpoint Security 10.6.1/10.7 February 2020 Update.

Security	ENSW-98874	Endpoint Security Firewall rules now correctly accepts executables when only signer details, hash, and file description are provided.

Web Control

Component	Reference	Resolution
Feature Fix	ENSW-26106	Resolved an issue where an Excel add-in didn't function with Web Control installed.
Feature Fix	ENSW-95849	Corrected the Severity mapping of Self Protection Rule Violation Threat event.
Installation	ENSW-97269	The system corruption and data deletion issue while uninstalling McAfee® Endpoint Security Web Control is now fixed.