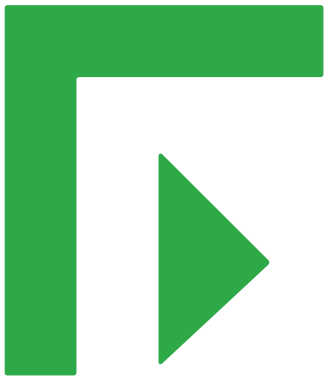

FORCEPOINT

Sidewinder

Release Notes

7.0.1.03H16

Revision A

Contents

- About this release on page 2
- Resolved issues on page 3
- Installation notes on page 5
- Known issues on page 5
- Find product documentation on page 6

About this release

This document contains important information about the current release. We strongly recommend that you read the entire document.

Forcepoint Sidewinder version 7.0.1.03H16 resolves issues present in the previous release.

Note: We have rebranded Sidewinder (formerly McAfee Firewall Enterprise) and the Sidewinder product documentation.

Supported firewall types

Sidewinder supports these firewall types.

- Forcepoint Sidewinder appliances
- Forcepoint Sidewinder, Virtual Appliance

Compatible products

Sidewinder is compatible with the following products.

- Forcepoint Sidewinder Control Center

For more information, see Knowledge Base article 9275 and the Technical Note *Using Firewall Enterprise with other McAfee products* at https://support.forcepoint.com.

Requirements

Before you install this version, make sure the Admin Console and Sidewinder requirements are met. For more information, see the *McAfee Firewall Enterprise Release Notes*, version 7.0.1.03.

In addition to the operating systems listed in the *Admin Console requirements* section of the *McAfee Firewall Enterprise Release Notes*, version 7.0.1.03, we also support:

- Windows 8

- Windows 10

Note: Windows 8 and Windows 10 are supported in traditional desktop mode. Tablet mode is not supported. Touchscreen is not supported.

Resolved issues

These issues are resolved in this release of the product. For a list of issues fixed in a previous release, see the Release Notes for the specific release.

Common Vulnerabilities and Exposures (CVEs)

BIND

- Imports a fix for CVE-2017-3145. See Knowledge Base article 15080 for more information. (1114795)

Kernel

- Tightens defenses against the Meltdown attack, CVE-2017-5754. This change also mitigates CVE-2017-5715 and CVE-2017-5753.
  This change prevents execution of programs not published by Forcepoint by disallowing binaries of the type "scrp" from being executed, which a rogue administrator (Admn) could have done previously. Scripts are still allowed with the type "scrp".

  This change also provides detection of a Meltdown attack in progress, killing the offending program and auditing that the attack occurred. This change has no performance impact. See Knowledge Base article 14992 for more information. (1114841)

NTP

- Upgrades NTP to version 4.2.8p11.
- Imports fixes for the following CVEs:

  ```
  CVE-2016-1549, CVE-2018-7170, CVE-2018-7182, CVE-2018-7183, CVE-2018-7184, and CVE-2018-7185.
  ```

  (1114853)

OpenSSH

- Imports a fix for CVE-2017-15906. (1114799)

OpenSSL

- Upgrades to OpenSSL 1.0.2o.
- Imports fixes for the following CVEs:

  ```
  CVE-2016-8610, CVE-2017-3735, CVE-2017-3736, CVE-2017-3737, CVE-2017-3738, CVE-2018-0733,
  and CVE-2018-0739.
  ```

  See Knowledge Base article 14990 and Knowledge Base article 15825 for more information. (1114775, 1114887, 1114888, 1114890, and 1114920)

tcpdump

- Upgrades to tcpdump version 4.9.2.

- Imports fixes for the following CVEs:

```
CVE-2017-11108, CVE-2017-11541, CVE-2017-11542, CVE-2017-11543, CVE-2017-11544, CVE-2017-11545,
CVE-2017-12893, CVE-2017-12894, CVE-2017-12895, CVE-2017-12896, CVE-2017-12897, CVE-2017-12898,
CVE-2017-12899, CVE-2017-12900, CVE-2017-12901, CVE-2017-12902, CVE-2017-12985, CVE-2017-12986,
CVE-2017-12987, CVE-2017-12988, CVE-2017-12989, CVE-2017-12990, CVE-2017-12991, CVE-2017-12992,
CVE-2017-12993, CVE-2017-12994, CVE-2017-12995, CVE-2017-12996, CVE-2017-12997, CVE-2017-12998,
CVE-2017-12999, CVE-2017-13000, CVE-2017-13001, CVE-2017-13002, CVE-2017-13003, CVE-2017-13004,
CVE-2017-13005, CVE-2017-13006, CVE-2017-13007, CVE-2017-13008, CVE-2017-13009, CVE-2017-13010,
CVE-2017-13011, CVE-2017-13012, CVE-2017-13013, CVE-2017-13014, CVE-2017-13015, CVE-2017-13016,
CVE-2017-13017, CVE-2017-13018, CVE-2017-13019, CVE-2017-13020, CVE-2017-13021, CVE-2017-13022,
CVE-2017-13023, CVE-2017-13024, CVE-2017-13025, CVE-2017-13026, CVE-2017-13027, CVE-2017-13028,
CVE-2017-13029, CVE-2017-13030, CVE-2017-13031, CVE-2017-13032, CVE-2017-13033, CVE-2017-13034,
CVE-2017-13035, CVE-2017-13036, CVE-2017-13037, CVE-2017-13038, CVE-2017-13039, CVE-2017-13040,
CVE-2017-13041, CVE-2017-13042, CVE-2017-13043, CVE-2017-13044, CVE-2017-13045, CVE-2017-13046,
CVE-2017-13047, CVE-2017-13048, CVE-2017-13049, CVE-2017-13050, CVE-2017-13051, CVE-2017-13052,
CVE-2017-13053, CVE-2017-13054, CVE-2017-13055, CVE-2017-13687, CVE-2017-13688, CVE-2017-13689,
CVE-2017-13690, CVE-2017-13725, and CVE-2017-16808.
```

  (1114786, 1114787, 1114788, 1114789, 1114790, 1114791, 1114792, 1114793, and 1114794)

telnetd

- Imports a fix for CVE-2016-1888. (1114838)

General Maintenance Changes

Admin Console

- Upgrades OpenSSL in the Admin Console. (1114816)
- Fixes a buffer overrun in cobrad. (1114944)

Audit

- Improves the performance of rollaudit. (1114516)

BIND

- Upgrades BIND to version 9.11.2-P1. (1114811, 1114854, and 1114889)
- Fixes named-internet error connecting to zone not allowed. (1114922)

Certificate management

- Changes several cmd error audits to debug audits. (1114796)
- Corrects an issue with accessing freed memory. (1114812)

Control Center

- Fixes Type Enforcement errors generated when attempting to verify a cluster using Control Center. (1114971)

Diagnostic tool

- Adds handling for the case where multiple core output is enabled. Includes the core for the given PID. Adds audit.raw to the diagnostic output so audit can be filtered. Adds top output to the diagnostic output. (1114931)

entrelayd

- Corrects an issue that could cause entrelayd to utilize high CPU cycles. (1114987)

Kernel

- Fixes an issue caused by a locking error when closing IPsec key socket. (1114947)

Package Management

- To make management of obsolete packages easier, cf package list makes it clearer which packages can be removed and which cannot. (1114758)
- A new cf package autoremove command has been added. The command removes all obsolete packages from the firewall. (1114758)
- Corrects an issue where uninstalling a patch incorrectly changes the status of patches that were made obsolete by the removed patch. (805688)
- Removes a warning about /vcdrom/packages/upscripts when running "cf package autoremove". (1114968)

Proxies

- Fixes memory leaks and an issue with rekeying in the SSH proxy. (1114778)
- Corrects an issue that could cause the HTTP proxy to utilize high CPU cycles. (1114948 and 1114955)
- Improves proxy session destruction process when proxy antivirus is enabled. (1114949)

Sendmail

- Corrects an issue where sendmail can spin up thousands of processes because of a misconfigured firewall admin email address that gets a "non-reachable" reply from DNS. (1114886, 1114905, and 1114963)
- Changes the sendmail default for Diffie-Hellman (DH) from 1024 to 2048 bits. (1114211)

Virtual appliance

- Enables Sidewinder on ESXi 6.0/VM Version 11. (1114767)

Miscellaneous

- Updates Forcepoint copyright year to 2018. (1114976)
- Removees the SSLv2, 40 bit, and 56 bit cipher choices from HTTPS Application defense and cf to match previous OpenSSL changes that were included in 7.0.1.03.H14. (1114193)

Installation notes

To bring your firewall to the latest patch version, follow the patch installation process appropriate for your environment.

Before you begin

The firewall must be at version 7.0.1.03H15.

- **Standalone or HA cluster** — See the *Forcepoint Sidewinder Administration Guide*.
- **Firewall or HA cluster managed by Control Center** — See the *Forcepoint Sidewinder Control Center Release Notes* and *Forcepoint Sidewinder Control Center Product Guide*.

Note: If your firewall is managed by Control Center, it must be at version 5.1.2 or later to manage firewalls at version 7.0.1.03H16.

Known issues

For a list of known issues in this product release, see Knowledge Base article 9386.

Find product documentation

On the Forcepoint support website, you can find information about a released product, including product documentation, technical articles, and more.

You can get additional information and support for your product on the Forcepoint support website at https://support.forcepoint.com. There, you can access product documentation, Knowledge Base articles, downloads, cases, and contact information.

Product documentation

Every Forcepoint product has a comprehensive set of documentation.

Sidewinder documentation includes:

Typical documents

- *Forcepoint Sidewinder Product Guide*
- *Forcepoint Sidewinder Release Notes*
- *Forcepoint Sidewinder Command Line Interface Reference Guide*
- *McAfee Firewall Enterprise ePolicy Orchestrator Extension Integration Guide*
- Technical Note — *Using Firewall Enterprise with other McAfee products*
- Application Note — *Configuring Department of Defense Common Access Card Authentication on Firewall Enterprise*

Hardware

- *McAfee Firewall Enterprise on Crossbeam X-Series Platforms Installation Guide*
- *Forcepoint Sidewinder, Virtual Appliance Installation Guide*
- *Forcepoint Sidewinder, Virtual Appliance Evaluation for Desktop Installation Guide*
- *Forcepoint Sidewinder Quick Start Guide*
- *Forcepoint Sidewinder Hardware Guide*, models S4016, 1402-C3, S5032, S6032, and S7032
- *Forcepoint Sidewinder Hardware Guide*, models S1104, S2008, and S3008

Certification

- *Firewall Enterprise Common Criteria Evaluated Configuration Guide*
- *Firewall Enterprise FIPS 140-2 Configuration Guide*
- *Firewall Enterprise FIPS 140-2 Level 2 Kit Installation Guide*, S models