Release Notes for AsyncOS 8.5.7 Hot Patch 3 for Cisco Email Security Appliances

Published: February 2, 2017
Revised: February 8, 2017

Contents

- What’s New, page 2
- Upgrade Paths, page 1
- Additional Information, page 3
- Additional Information, page 3
- Service and Support, page 4
## What’s New

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Duplicate Boundaries Verification</td>
<td>Cisco Email Security appliance can now detect messages with duplicate MIME boundaries and perform actions on them. Use the Duplicate Boundaries Verification content filter condition or the <code>duplicate_boundaries</code> message filter rule to detect messages with duplicate MIME boundaries.</td>
</tr>
</tbody>
</table>

**Example**

The following message filter will quarantine all the messages that contain duplicate MIME boundaries.

```plaintext
DuplicateBoundaries: if (duplicate_boundaries) {
    quarantine("Policy");
}
```

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
</table>
| Message Filter Rule to Detect Malformed MIME Headers | You can now take actions on messages with malformed MIME headers using the new message filter rule: “`malformed-header`.” The following example shows how to quarantine all the messages with malformed MIME headers:

```plaintext
quarantine_malformed_headers: if (malformed-header) {
    quarantine("Policy");
}
``` |

## Upgrade Paths

You can upgrade to release 8.5.7-104 from 8.5.7-043 version.

## Known and Fixed Issues

Use the Cisco Bug Search Tool to find information about known and fixed defects in this release.

- Bug Search Tool Requirements, page 2
- Lists of Known and Fixed Issues, page 3
- Finding Information about Known and Resolved Issues, page 3

## Bug Search Tool Requirements

Lists of Known and Fixed Issues

<table>
<thead>
<tr>
<th>Known Issues</th>
<th>Fixed Issues</th>
</tr>
</thead>
</table>

Finding Information about Known and Resolved Issues

Use the Cisco Bug Search Tool to find the most current information about known and resolved defects.

Before You Begin

Register for a Cisco account if you do not have one. Go to https://tools.cisco.com/RPF/register/register.do.

Procedure

Step 1 Go to https://tools.cisco.com/bugsearch/.
Step 2 Log in with your Cisco account credentials.
Step 3 Click Select from list > Security > Email Security > Cisco Email Security Appliance, and click OK.
Step 4 In Releases field, enter the version of the release, for example, 8.5.7-104.
Step 5 Depending on your requirements, do one of the following:
   • To view the list of resolved issues, select Fixed in these Releases from the Show Bugs drop down.
   • To view the list of known issues, select Affecting these Releases from the Show Bugs drop down and select Open from the Status drop down.

Note

If you have questions or problems, click the Help or Feedback links at the top right side of the tool. There is also an interactive tour; to view it, click the link in the orange bar above the search fields.

Additional Information

Service and Support

For service and support information for Cisco Content Security appliances, see:


If you purchased support through a reseller or another supplier, please contact that supplier directly with your product support issues.

For noncritical questions and issues, you can also submit a customer support request from the appliance. For instructions, see the User Guide or online help.