



# CVE-2016-1368

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

## Summary

|                        |                                                                                                                    |
|------------------------|--------------------------------------------------------------------------------------------------------------------|
| <b>CVE</b>             | CVE-2016-1368                                                                                                      |
| <b>State</b>           | PUBLISHED                                                                                                          |
| <b>Assigner</b>        | cisco                                                                                                              |
| <b>Source Priority</b> | CVE Program / NVD first with legacy fallback                                                                       |
| <b>Published</b>       | 2016-05-05 21:59:00 UTC                                                                                            |
| <b>Updated</b>         | 2026-05-06 22:30:45 UTC                                                                                            |
| <b>Description</b>     | Cisco FirePOWER System Software 5.3.x through 5.3.0.6 and 5.4.x through 5.4.0.3 on FirePOWER 7000 and 8000 appliar |

## Risk And Classification

**Primary CVSS:** v3.0 7.5 HIGH from nvd@nist.gov

CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

**Problem Types:** CWE-399 | n/a

| Version | Source       | Type    | Score | Severity | Vector                                       |
|---------|--------------|---------|-------|----------|----------------------------------------------|
| 3.0     | nvd@nist.gov | Primary | 7.5   | HIGH     | CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H |
| 2.0     | nvd@nist.gov | Primary | 7.8   |          | AV:N/AC:L/Au:N/C:N/I:N/A:C                   |

## CVSS v3.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

None

Integrity

None

Availability

High

CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

None

Integrity

None

Availability

Complete

AV:N/AC:L/Au:N/C:N/I:N/A:C

| NVD Known Affected Configurations (CPE 2.3) |        |                           |         |        |         |          |
|---------------------------------------------|--------|---------------------------|---------|--------|---------|----------|
| Type                                        | Vendor | Product                   | Version | Update | Edition | Language |
| Application                                 | Cisco  | Firesight System Software | 5.2.0   | All    | All     | All      |
| Application                                 | Cisco  | Firesight System Software | 5.2.0.1 | All    | All     | All      |
| Application                                 | Cisco  | Firesight System Software | 5.2.0.2 | All    | All     | All      |
| Application                                 | Cisco  | Firesight System Software | 5.2.0.3 | All    | All     | All      |
| Application                                 | Cisco  | Firesight System Software | 5.2.0.4 | All    | All     | All      |
| Application                                 | Cisco  | Firesight System Software | 5.2.0.5 | All    | All     | All      |
| Application                                 | Cisco  | Firesight System Software | 5.2.0.6 | All    | All     | All      |
| Application                                 | Cisco  | Firesight System Software | 5.2.0.8 | All    | All     | All      |
| Application                                 | Cisco  | Firesight System Software | 5.3.0   | All    | All     | All      |
| Application                                 | Cisco  | Firesight System Software | 5.3.0.1 | All    | All     | All      |
| Application                                 | Cisco  | Firesight System Software | 5.3.0.2 | All    | All     | All      |
| Application                                 | Cisco  | Firesight System Software | 5.3.0.3 | All    | All     | All      |
| Application                                 | Cisco  | Firesight System Software | 5.3.0.4 | All    | All     | All      |
| Application                                 | Cisco  | Firesight System Software | 5.3.0.5 | All    | All     | All      |
| Application                                 | Cisco  | Firesight System Software | 5.3.0.6 | All    | All     | All      |
| Application                                 | Cisco  | Firesight System Software | 5.3.0.7 | All    | All     | All      |
| Application                                 | Cisco  | Firesight System Software | 5.3.1   | All    | All     | All      |

|             |       |                           |         |     |     |     |
|-------------|-------|---------------------------|---------|-----|-----|-----|
| Application | Cisco | Firesight System Software | 5.3.1.1 | All | All | All |
| Application | Cisco | Firesight System Software | 5.3.1.2 | All | All | All |
| Application | Cisco | Firesight System Software | 5.3.1.3 | All | All | All |
| Application | Cisco | Firesight System Software | 5.3.1.4 | All | All | All |
| Application | Cisco | Firesight System Software | 5.3.1.5 | All | All | All |
| Application | Cisco | Firesight System Software | 5.3.1.6 | All | All | All |
| Application | Cisco | Firesight System Software | 5.3.1.7 | All | All | All |
| Application | Cisco | Firesight System Software | 5.4.0   | All | All | All |
| Application | Cisco | Firesight System Software | 5.4.0.1 | All | All | All |
| Application | Cisco | Firesight System Software | 5.4.0.2 | All | All | All |
| Application | Cisco | Firesight System Software | 5.4.0.3 | All | All | All |

| Vendor Declared Affected Products |        |         |              |               |  |
|-----------------------------------|--------|---------|--------------|---------------|--|
| Source                            | Vendor | Product | Version      | Platforms     |  |
| CNA                               | Na     | N/a     | affected n/a | Not specified |  |

| References                                                                        |                                      |                         |
|-----------------------------------------------------------------------------------|--------------------------------------|-------------------------|
| Reference                                                                         | Source                               | Link                    |
| Cisco FirePOWER System Software Packet Processing Denial of Service Vulnerability | af854a3a-2127-422b-91ae-364da2661108 | <a href="#">tools.c</a> |
| CVE Program record                                                                | CVE.ORG                              | <a href="#">www.c</a>   |
| NVD vulnerability detail                                                          | NVD                                  | <a href="#">nvd.nis</a> |

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.