



# CVE-2006-2054

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2006-2054
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2006-04-26 20:06:00 UTC
<b>Updated</b>	2017-07-20 01:31:00 UTC
<b>Description</b>	3Com Baseline Switch 2848-SFP Plus Model #3C16486 with firmware before 1.0.2.0 allows remote attackers to cause a de

## Risk And Classification

**Problem Types:** NVD-CWE-Other

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	3com	3c16486	All	All	All	All

## References

Reference	Source
3Com Baseline Switch 2848-SFP Plus Lets Remote Users Deny Service With Specially Crafted DHCP Packets - SecurityTracker	SECTRA
404 Error   HPE	CONFIRM
Secunia - Advisories - 3Com Baseline Switch 2848-SFP DHCP Potential Denial of Service	SECUNIA
IBM X-Force Exchange	XF
24942	OSVDB
3Com Baseline Switch 2848-SFP Plus Remote Denial Of Service Vulnerability	BID
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

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

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

**CVE.report and Source URL Uptime Status** [status.cve.report](#)