



CVE-2007-3701

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

CVE	CVE-2007-3701
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2007-07-11 23:30:00 UTC
Updated	2018-10-15 21:29:00 UTC
Description	<p>TipingPoint IPS before 20070710 does not properly handle a hex-encoded alternate Unicode '/' (slash) character, which m</p>

Risk And Classification

Problem Types: CWE-20

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	3com	Tippingpoint Ips Tos	2.1	All	All	All
Operating System	3com	Tippingpoint Ips Tos	2.1.4.6324	All	All	All
Operating System	3com	Tippingpoint Ips Tos	2.2	All	All	All
Operating System	3com	Tippingpoint Ips Tos	2.2.1	All	All	All
Operating System	3com	Tippingpoint Ips Tos	2.2.1.6506	All	All	All
Operating System	3com	Tippingpoint Ips Tos	2.2.2	All	All	All
Operating System	3com	Tippingpoint Ips Tos	2.2.3	All	All	All
Operating System	3com	Tippingpoint Ips Tos	2.2.4	All	All	All
Operating System	3com	Tippingpoint Ips Tos	2.5	All	All	All
Operating System	3com	Tippingpoint Ips Tos	2.5.1	All	All	All
Operating System	3com	Tippingpoint Ips Tos	2.1	All	All	All
Operating System	3com	Tippingpoint Ips Tos	2.1.4.6324	All	All	All
Operating System	3com	Tippingpoint Ips Tos	2.2	All	All	All
Operating System	3com	Tippingpoint Ips Tos	2.2.1	All	All	All
Operating System	3com	Tippingpoint Ips Tos	2.2.1.6506	All	All	All
Operating System	3com	Tippingpoint Ips Tos	2.2.2	All	All	All
Operating System	3com	Tippingpoint Ips Tos	2.2.3	All	All	All

Operating System	3com	Tippingpoint Ips Tos	2.2.4	All	All	All
Operating System	3com	Tippingpoint Ips Tos	2.5	All	All	All
Operating System	3com	Tippingpoint Ips Tos	2.5.1	All	All	All
Application	Tippingpoint	Tipping Point	1200	All	All	All
Application	Tippingpoint	Tipping Point	1200e	All	All	All
Application	Tippingpoint	Tipping Point	200	All	All	All
Application	Tippingpoint	Tipping Point	200e	All	All	All
Application	Tippingpoint	Tipping Point	2400e	All	All	All
Application	Tippingpoint	Tipping Point	400	All	All	All
Application	Tippingpoint	Tipping Point	50	All	All	All
Application	Tippingpoint	Tipping Point	5000e	All	All	All
Application	Tippingpoint	Tipping Point	600e	All	All	All
Application	Tippingpoint	Tipping Point	sms	All	All	All
Application	Tippingpoint	Tipping Point	x505	All	All	All
Application	Tippingpoint	Tipping Point	x506	All	All	All
Application	Tippingpoint	Tipping Point	zpha	All	All	All
Application	Tippingpoint	Tipping Point	1200	All	All	All
Application	Tippingpoint	Tipping Point	1200e	All	All	All
Application	Tippingpoint	Tipping Point	200	All	All	All
Application	Tippingpoint	Tipping Point	200e	All	All	All
Application	Tippingpoint	Tipping Point	2400e	All	All	All
Application	Tippingpoint	Tipping Point	400	All	All	All
Application	Tippingpoint	Tipping Point	50	All	All	All
Application	Tippingpoint	Tipping Point	5000e	All	All	All
Application	Tippingpoint	Tipping Point	600e	All	All	All
Application	Tippingpoint	Tipping Point	sms	All	All	All
Application	Tippingpoint	Tipping Point	x505	All	All	All
Application	Tippingpoint	Tipping Point	x506	All	All	All
Application	Tippingpoint	Tipping Point	zpha	All	All	All

References

Reference	Source
Risks in POS Systems: The Importance of a Security Assessment	M
3Com TippingPoint IPS Extended Unicode Detection Bypass - Advisories - Secunia	SI
IBM X-Force Exchange	XI

3Com Security Alert: 3COM-07-003	CI
35970	O
TippingPoint IPS Unicode Character Detection Bypass Vulnerability	BI
TippingPoint Intrusion Prevention System Alternate Unicode Character Encodings Lets Remote Users Evade Detection - SecurityTracker	SI
SecurityFocus	BI
[Full-Disclosure] Mailing List Charter	FI
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VI
CVE Program record	C
NVD vulnerability detail	N

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](#)