CVE-2005-1267

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2005-1267
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2005-06-10 04:00:00 UTC
Updated	2018-10-19 15:31:00 UTC
Description	The bgp_update_print function in tcpdump 3.x does not properly handle a -1 return value from the decode_prefix4 function,

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Gentoo	Linux	All	All	All	All
Operating System	Gentoo	Linux	All	All	All	All
Application	Lbl	Tcpdump	3.4	All	All	All
Application	Lbl	Tcpdump	3.4a6	All	All	All
Application	Lbl	Tcpdump	3.5	All	All	All
Application	Lbl	Tcpdump	3.5.2	All	All	All
Application	Lbl	Tcpdump	3.5_alpha	All	All	All
Application	Lbl	Tcpdump	3.6.2	All	All	All
Application	Lbl	Tcpdump	3.6.3	All	All	All
Application	Lbl	Tcpdump	3.7	All	All	All
Application	Lbl	Tcpdump	3.7.1	All	All	All
Application	Lbl	Tcpdump	3.7.2	All	All	All
Application	Lbl	Tcpdump	3.8.1	All	All	All
Application	Lbl	Tcpdump	3.8.2	All	All	All
Application	Lbl	Tcpdump	3.8.3	All	All	All
Application	Lbl	Tcpdump	3.9	All	All	All
Application	Lbl	Tcpdump	3.9.1	All	All	All

Application	Lbl	Tcpdump	3.4	All	All	All
Application	Lbl	Tcpdump	3.4a6	All	All	All
Application	Lbl	Tcpdump	3.5	All	All	All
Application	Lbl	Tcpdump	3.5.2	All	All	All
Application	Lbl	Tcpdump	3.5_alpha	All	All	All
Application	Lbl	Tcpdump	3.6.2	All	All	All
Application	Lbl	Tcpdump	3.6.3	All	All	All
Application	Lbl	Tcpdump	3.7	All	All	All
Application	Lbl	Tcpdump	3.7.1	All	All	All
Application	Lbl	Tcpdump	3.7.2	All	All	All
Application	Lbl	Tcpdump	3.8.1	All	All	All
Application	Lbl	Tcpdump	3.8.2	All	All	All
Application	Lbl	Tcpdump	3.8.3	All	All	All
Application	Lbl	Tcpdump	3.9	All	All	All
Application	Lbl	Tcpdump	3.9.1	All	All	All
Operating System	Mandrakesoft	Mandrake Linux	10.1	All	All	All
Operating System	Mandrakesoft	Mandrake Linux	10.1	All	x86_64	All
Operating System	Mandrakesoft	Mandrake Linux	10.2	All	All	All
Operating System	Mandrakesoft	Mandrake Linux	10.2	All	x86_64	All
Operating System	Mandrakesoft	Mandrake Linux	10.1	All	All	All
Operating System	Mandrakesoft	Mandrake Linux	10.1	All	x86_64	All
Operating System	Mandrakesoft	Mandrake Linux	10.2	All	All	All
Operating System	Mandrakesoft	Mandrake Linux	10.2	All	x86_64	All
Operating System	Redhat	Fedora Core	core_3.0	All	All	All
Operating System	Redhat	Fedora Core	core_4.0	All	All	All
Operating System	Redhat	Fedora Core	core_3.0	All	All	All
Operating System	Redhat	Fedora Core	core_4.0	All	All	All
Operating System	Trustix	Secure Linux	2.0	All	All	All
Operating System	Trustix	Secure Linux	2.1	All	All	All
Operating System	Trustix	Secure Linux	2.2	All	All	All
Operating System	Trustix	Secure Linux	2.0	All	All	All
Operating System	Trustix	Secure Linux	2.1	All	All	All
Operating System	Trustix	Secure Linux	2.2	All	All	All

References

Reference	Source	Link	Tags
[SECURITY] Fedora Core 3 Update: tcpdump-3.8.2-9.FC3	FEDORA	www.redhat.com	Patch, Vendor Advisory
Secunia - Advisories - tcpdump BGP Denial of Service Vulnerability	SECUNIA	secunia.com	Patch, Vendor Advisory
SecurityFocus	FEDORA	www.securityfocus.com	
Debian -- Security Information -- DSA-854-1 tcpdump	DEBIAN	www.debian.org	
2005-0028	TRUSTIX	www.trustix.org	Patch, Vendor Advisory
Secunia - Advisories - Debian update for tcpdump	SECUNIA	secunia.com	
159208 – CAN-2005-1267 tcpdump BGP DoS	MISC	bugzilla.redhat.com	Patch, Vendor Advisory
tcpdump BGP Decoding Routines Denial Of Service Vulnerability	BID	www.securityfocus.com	
rhn.redhat.com | Red Hat Support	REDHAT	www.redhat.com	
Repository / Oval Repository	OVAL	oval.cisecurity.org	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

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