



CVE-2006-0804

Published on: 02/20/2006 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:25:06 PM UTC

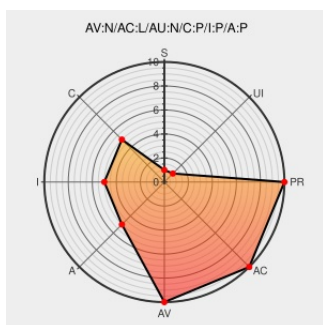
CVE-2006-0804

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



Certain versions of [Tin](#) from [Tin](#) contain the following vulnerability:

Off-by-one error in TIN 1.8.0 and earlier might allow attackers to execute arbitrary code via unknown vectors that trigger a buffer overflow.

CVE-2006-0804 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **7.5 - HIGH**

Access
Vector

NETWORK

Access
Complexity

LOW

Authentication

NONE

Confidentiality
Impact

PARTIAL

Integrity
Impact

PARTIAL

Availability
Impact

PARTIAL

CVE References

Description

OpenPKG Meta: SiteMap

Tags

[Vendor Advisory](#)
[www.openpkg.org](#)
[text/html](#)

Link

[OPENPKG OpenPKG-SA-2006.005](#)

Security Announcement

[web.archive.org](#)
[text/html](#)
[Inactive Link](#) [Not Archived](#)

[SUSE SUSE-SR:2006:005](#)

Tin News Reader Buffer Overflow Vulnerability

[cve.report \(archive\)](#)
[text/html](#)

[BID 16728](#)

Webmail : Solution de messagerie professionnelle - OVHcloud-OVH

[www.vupen.com](#)
[text/html](#)

[VUPEN ADV-2006-0702](#)

IBM X-Force Exchange

[exchange.xforce.ibmcloud.com](#)
[text/html](#)

[XF tin-offbyone-bo\(24841\)](#)

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Tin	Tin	1.0_pl0	All	All	All
Application	Tin	Tin	1.0_pl1	All	All	All
Application	Tin	Tin	1.0_pl2	All	All	All
Application	Tin	Tin	1.0_pl3	All	All	All
Application	Tin	Tin	1.0_pl4	All	All	All
Application	Tin	Tin	1.0_pl5	All	All	All
Application	Tin	Tin	1.1_pl0	All	All	All
Application	Tin	Tin	1.1_pl1	All	All	All
Application	Tin	Tin	1.1_pl2	All	All	All
Application	Tin	Tin	1.1_pl3	All	All	All
Application	Tin	Tin	1.1_pl4	All	All	All
Application	Tin	Tin	1.1_pl5	All	All	All
Application	Tin	Tin	1.1_pl6	All	All	All
Application	Tin	Tin	1.1_pl7	All	All	All
Application	Tin	Tin	1.1_pl8	All	All	All
Application	Tin	Tin	1.1_pl9	All	All	All
Application	Tin	Tin	1.2_pl0	All	All	All
Application	Tin	Tin	1.2_pl1	All	All	All
Application	Tin	Tin	1.2_pl2	All	All	All
Application	Tin	Tin	1.4.0	All	All	All
Application	Tin	Tin	1.4.1	All	All	All
Application	Tin	Tin	1.4.2	All	All	All
Application	Tin	Tin	1.4.3	All	All	All
Application	Tin	Tin	1.4.4	All	All	All
Application	Tin	Tin	1.4.5	All	All	All

Application	Tin	Tin	1.4.6	All	All	All
Application	Tin	Tin	1.4.7	All	All	All
Application	Tin	Tin	1.6.0	All	All	All
Application	Tin	Tin	1.6.1	All	All	All
Application	Tin	Tin	1.6.2	All	All	All
Application	Tin	Tin	1.8.0	All	All	All
Application	Tin	Tin	1.0_pl0	All	All	All
Application	Tin	Tin	1.0_pl1	All	All	All
Application	Tin	Tin	1.0_pl2	All	All	All
Application	Tin	Tin	1.0_pl3	All	All	All
Application	Tin	Tin	1.0_pl4	All	All	All
Application	Tin	Tin	1.0_pl5	All	All	All
Application	Tin	Tin	1.1_pl0	All	All	All
Application	Tin	Tin	1.1_pl1	All	All	All
Application	Tin	Tin	1.1_pl2	All	All	All
Application	Tin	Tin	1.1_pl3	All	All	All
Application	Tin	Tin	1.1_pl4	All	All	All
Application	Tin	Tin	1.1_pl5	All	All	All
Application	Tin	Tin	1.1_pl6	All	All	All
Application	Tin	Tin	1.1_pl7	All	All	All
Application	Tin	Tin	1.1_pl8	All	All	All
Application	Tin	Tin	1.1_pl9	All	All	All
Application	Tin	Tin	1.2_pl0	All	All	All
Application	Tin	Tin	1.2_pl1	All	All	All
Application	Tin	Tin	1.2_pl2	All	All	All
Application	Tin	Tin	1.4.0	All	All	All
Application	Tin	Tin	1.4.1	All	All	All
Application	Tin	Tin	1.4.2	All	All	All
Application	Tin	Tin	1.4.3	All	All	All
Application	Tin	Tin	1.4.4	All	All	All
Application	Tin	Tin	1.4.5	All	All	All
Application	Tin	Tin	1.4.6	All	All	All
Application	Tin	Tin	1.4.7	All	All	All
Application	Tin	Tin	1.6.0	All	All	All
Application	Tin	Tin	1.6.1	All	All	All

Application	Tin	Tin	1.6.2	All	All	All
Application	Tin	Tin	1.8.0	All	All	All
cpe:2.3:a:tin:tin:1.0_pl0:*****:						
cpe:2.3:a:tin:tin:1.0_pl1:*****:						
cpe:2.3:a:tin:tin:1.0_pl2:*****:						
cpe:2.3:a:tin:tin:1.0_pl3:*****:						
cpe:2.3:a:tin:tin:1.0_pl4:*****:						
cpe:2.3:a:tin:tin:1.0_pl5:*****:						
cpe:2.3:a:tin:tin:1.1_pl0:*****:						
cpe:2.3:a:tin:tin:1.1_pl1:*****:						
cpe:2.3:a:tin:tin:1.1_pl2:*****:						
cpe:2.3:a:tin:tin:1.1_pl3:*****:						
cpe:2.3:a:tin:tin:1.1_pl4:*****:						
cpe:2.3:a:tin:tin:1.1_pl5:*****:						
cpe:2.3:a:tin:tin:1.1_pl6:*****:						
cpe:2.3:a:tin:tin:1.1_pl7:*****:						
cpe:2.3:a:tin:tin:1.1_pl8:*****:						
cpe:2.3:a:tin:tin:1.1_pl9:*****:						
cpe:2.3:a:tin:tin:1.2_pl0:*****:						
cpe:2.3:a:tin:tin:1.2_pl1:*****:						
cpe:2.3:a:tin:tin:1.2_pl2:*****:						
cpe:2.3:a:tin:tin:1.4.0:*****:						
cpe:2.3:a:tin:tin:1.4.1:*****:						
cpe:2.3:a:tin:tin:1.4.2:*****:						
cpe:2.3:a:tin:tin:1.4.3:*****:						
cpe:2.3:a:tin:tin:1.4.4:*****:						
cpe:2.3:a:tin:tin:1.4.5:*****:						
cpe:2.3:a:tin:tin:1.4.6:*****:						
cpe:2.3:a:tin:tin:1.4.7:*****:						

cpe:2.3:a:tin:tin:1.6.0:~::~~::~~::~~::~~::~~::~~:::
cpe:2.3:a:tin:tin:1.6.1:~::~~::~~::~~::~~::~~::~~:::
cpe:2.3:a:tin:tin:1.6.2:~::~~::~~::~~::~~::~~::~~:::
cpe:2.3:a:tin:tin:1.8.0:~::~~::~~::~~::~~::~~::~~:::
cpe:2.3:a:tin:tin:1.0_pl0:~::~~::~~::~~::~~::~~::~~:::
cpe:2.3:a:tin:tin:1.0_pl1:~::~~::~~::~~::~~::~~::~~:::
cpe:2.3:a:tin:tin:1.0_pl2:~::~~::~~::~~::~~::~~::~~:::
cpe:2.3:a:tin:tin:1.0_pl3:~::~~::~~::~~::~~::~~::~~:::
cpe:2.3:a:tin:tin:1.0_pl4:~::~~::~~::~~::~~::~~::~~:::
cpe:2.3:a:tin:tin:1.0_pl5:~::~~::~~::~~::~~::~~::~~:::
cpe:2.3:a:tin:tin:1.1_pl0:~::~~::~~::~~::~~::~~::~~:::
cpe:2.3:a:tin:tin:1.1_pl1:~::~~::~~::~~::~~::~~::~~:::
cpe:2.3:a:tin:tin:1.1_pl2:~::~~::~~::~~::~~::~~::~~:::
cpe:2.3:a:tin:tin:1.1_pl3:~::~~::~~::~~::~~::~~::~~:::
cpe:2.3:a:tin:tin:1.1_pl4:~::~~::~~::~~::~~::~~::~~:::
cpe:2.3:a:tin:tin:1.1_pl5:~::~~::~~::~~::~~::~~::~~:::
cpe:2.3:a:tin:tin:1.1_pl6:~::~~::~~::~~::~~::~~::~~:::
cpe:2.3:a:tin:tin:1.1_pl7:~::~~::~~::~~::~~::~~::~~:::
cpe:2.3:a:tin:tin:1.1_pl8:~::~~::~~::~~::~~::~~::~~:::
cpe:2.3:a:tin:tin:1.1_pl9:~::~~::~~::~~::~~::~~::~~:::
cpe:2.3:a:tin:tin:1.2_pl0:~::~~::~~::~~::~~::~~::~~:::
cpe:2.3:a:tin:tin:1.2_pl1:~::~~::~~::~~::~~::~~::~~:::
cpe:2.3:a:tin:tin:1.2_pl2:~::~~::~~::~~::~~::~~::~~:::
cpe:2.3:a:tin:tin:1.4.0:~::~~::~~::~~::~~::~~::~~:::
cpe:2.3:a:tin:tin:1.4.1:~::~~::~~::~~::~~::~~::~~:::
cpe:2.3:a:tin:tin:1.4.2:~::~~::~~::~~::~~::~~::~~:::
cpe:2.3:a:tin:tin:1.4.3:~::~~::~~::~~::~~::~~::~~:::
cpe:2.3:a:tin:tin:1.4.4:~::~~::~~::~~::~~::~~::~~:::

cpe:2.3:a:tin:tin:1.4.5:*****:
cpe:2.3:a:tin:tin:1.4.6:*****:
cpe:2.3:a:tin:tin:1.4.7:*****:
cpe:2.3:a:tin:tin:1.6.0:*****:
cpe:2.3:a:tin:tin:1.6.1:*****:
cpe:2.3:a:tin:tin:1.6.2:*****:
cpe:2.3:a:tin:tin:1.8.0:*****:

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID→](#)