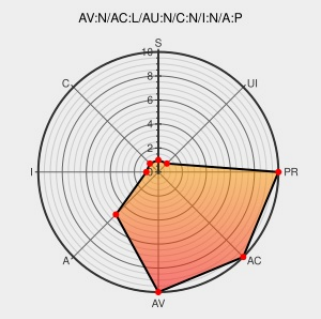
CVE-2004-1680

Published on: 09/13/2004 04:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:09 PM UTC

CVE-2004-1680

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Xpressa from Pingtel contain the following vulnerability:

application.cgi in the Pingtel Xpressa handset running firmware 2.1.11.24 allows remote authenticated users to cause a denial of service (VxWorks OS crash) via a long HTTP GET request, possibly triggering a buffer overflow.

CVE-2004-1680 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 5 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
NONE	NONE	PARTIAL

CVE References

Description	Tags	Link
IBM X-Force Exchange	exchange.xforce.ibmcloud.com, text/html	XF xpressa-applicationcgi-dos(17346)
Secunia - Advisories - Pingtel Xpressa HTTP Management Interface Denial of Service	Exploit, Patch, Vendor Advisory, web.archive.org, text/html	SECUNIA 12523
	Exploit, Patch, Vendor Advisory, www.atstake.com, text/plain, Inactive Link, Not Archived	ATSTAKE A091304-2
Pingtel Xpressa Handset Remote Denial Of Service Vulnerability	Exploit	BID 11161

Patch
Vendor Advisory
cve.report (archive)
text/html

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
Hardware	Pingtel	Xpressa	1.2.5	All	All	All
Hardware	Pingtel	Xpressa	1.2.7.4	All	All	All
Hardware	Pingtel	Xpressa	1.2.8	All	All	All
Hardware	Pingtel	Xpressa	2.0	All	All	All
Hardware	Pingtel	Xpressa	2.0.1	All	All	All
Hardware	Pingtel	Xpressa	2.1.11.24	All	All	All
Hardware	Pingtel	Xpressa	1.2.5	All	All	All
Hardware	Pingtel	Xpressa	1.2.7.4	All	All	All
Hardware	Pingtel	Xpressa	1.2.8	All	All	All
Hardware	Pingtel	Xpressa	2.0	All	All	All
Hardware	Pingtel	Xpressa	2.0.1	All	All	All
Hardware	Pingtel	Xpressa	2.1.11.24	All	All	All

cpe:2.3:h:pingtel:xpressa:1.2.5:*:*:*:*:*:*:*:

cpe:2.3:h:pingtel:xpressa:1.2.7.4:*:*:*:*:*:*:*:

cpe:2.3:h:pingtel:xpressa:1.2.8:*:*:*:*:*:*:*:

cpe:2.3:h:pingtel:xpressa:2.0:*:*:*:*:*:*:*:

cpe:2.3:h:pingtel:xpressa:2.0.1:*:*:*:*:*:*:*:

cpe:2.3:h:pingtel:xpressa:2.1.11.24:*:*:*:*:*:*:*:

cpe:2.3:h:pingtel:xpressa:1.2.5:*:*:*:*:*:*:*:

cpe:2.3:h:pingtel:xpressa:1.2.7.4:*:*:*:*:*:*:*:

cpe:2.3:h:pingtel:xpressa:1.2.8:*:*:*:*:*:*:*:

cpe:2.3:h:pingtel:xpressa:2.0:*:*:*:*:*:*:*:

cpe:2.3:h:pingtel:xpressa:2.0.1:*:*:*:*:*:*:*:

cpe:2.3:h:pingtel:xpressa:2.1.11.24:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→