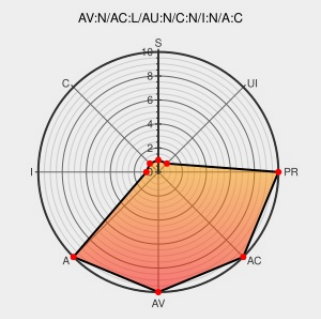
CVE-2006-2078

Published on: 04/27/2006 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:25:07 PM UTC

CVE-2006-2078

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



Certain versions of Fitelnet from Furukawa Electric contain the following vulnerability:

Multiple unspecified vulnerabilities in multiple FITELnet products, including FITELnet-F40, F80, F100, F120, F1000, and E20/E30, allow remote attackers to cause a denial of service via crafted DNS messages that trigger errors in (1) ProxyDNS or (2) PKI-Resolver, as demonstrated by the OUSPG PROTOS DNS test suite.

CVE-2006-2078 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 7.8 - HIGH

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

CVE References

Description	Tags	Link
Multiple FITELnet Products Unspecified DNS Handling Vulnerabilities	Patch, cve.report (archive), text/html	BID 17710
No Description Provided	www.furukawa.co.jp, text/html	CONFIRM www.furukawa.co.jp/fitelnet/topic/dns2_attacks.html
IBM X-Force Exchange	exchange.xforce.ibmcloud.com, text/html	XF dns-improper-request-handling(26081)
	Patch, Vendor Advisory, www.niscc.gov.uk, application/pdf, Inactive Link, Not Archived	MISC www.niscc.gov.uk/niscc/docs/re-20060425-00312.pdf?lang=en

No Description Provided	Patch web.archive.org text/html Inactive Link Not Archived	MISC www.niscc.gov.uk/niscc/docs/br-20060425-00311.html?lang=en
FITELnet Products DNS Handling Vulnerability - Advisories - Secunia	Patch Vendor Advisory web.archive.org text/html	SECUNIA 19820
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	www.vupen.com text/html	VUPEN ADV-2006-1536
Webmail - OVH	www.vupen.com text/html	VUPEN ADV-2006-1505
US-CERT Vulnerability Note VU#955777	US Government Resource www.kb.cert.org text/html	CERT-VN VU#955777

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Furukawa Electric	Fitelnet	e20	All	All	All
Hardware	Furukawa Electric	Fitelnet	e30	All	All	All
Hardware	Furukawa Electric	Fitelnet	f100	All	All	All
Hardware	Furukawa Electric	Fitelnet	f1000	All	All	All
Hardware	Furukawa Electric	Fitelnet	f120	All	All	All
Hardware	Furukawa Electric	Fitelnet	f3000	All	All	All
Hardware	Furukawa Electric	Fitelnet	f40	All	All	All
Hardware	Furukawa Electric	Fitelnet	f80	All	All	All
Hardware	Furukawa Electric	Fitelnet	e20	All	All	All
Hardware	Furukawa Electric	Fitelnet	e30	All	All	All
Hardware	Furukawa Electric	Fitelnet	f100	All	All	All
Hardware	Furukawa Electric	Fitelnet	f1000	All	All	All
Hardware	Furukawa Electric	Fitelnet	f120	All	All	All
Hardware	Furukawa Electric	Fitelnet	f3000	All	All	All
Hardware	Furukawa Electric	Fitelnet	f40	All	All	All

Hardware	Furukawa Electric	Fitelnet	f80	All	All	All
Hardware	Furukawa Electric	Mucho-ev Pk	All	All	All	All
Hardware	Furukawa Electric	Mucho-ev Pk	All	All	All	All

cpe:2.3:h:furukawa_electric:fitelnet:e20:*:*:*:*:*:*:*:

cpe:2.3:h:furukawa_electric:fitelnet:e30:*:*:*:*:*:*:*:

cpe:2.3:h:furukawa_electric:fitelnet:f100:*:*:*:*:*:*:*:

cpe:2.3:h:furukawa_electric:fitelnet:f1000:*:*:*:*:*:*:*:

cpe:2.3:h:furukawa_electric:fitelnet:f120:*:*:*:*:*:*:*:

cpe:2.3:h:furukawa_electric:fitelnet:f3000:*:*:*:*:*:*:*:

cpe:2.3:h:furukawa_electric:fitelnet:f40:*:*:*:*:*:*:*:

cpe:2.3:h:furukawa_electric:fitelnet:f80:*:*:*:*:*:*:*:

cpe:2.3:h:furukawa_electric:fitelnet:e20:*:*:*:*:*:*:*:

cpe:2.3:h:furukawa_electric:fitelnet:e30:*:*:*:*:*:*:*:

cpe:2.3:h:furukawa_electric:fitelnet:f100:*:*:*:*:*:*:*:

cpe:2.3:h:furukawa_electric:fitelnet:f1000:*:*:*:*:*:*:*:

cpe:2.3:h:furukawa_electric:fitelnet:f120:*:*:*:*:*:*:*:

cpe:2.3:h:furukawa_electric:fitelnet:f3000:*:*:*:*:*:*:*:

cpe:2.3:h:furukawa_electric:fitelnet:f40:*:*:*:*:*:*:*:

cpe:2.3:h:furukawa_electric:fitelnet:f80:*:*:*:*:*:*:*:

cpe:2.3:h:furukawa_electric:mucho-ev_pk:*:*:*:*:*:*:*:*:

cpe:2.3:h:furukawa_electric:mucho-ev_pk:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

CVE.report and Source URL Uptime Status status.cve.report