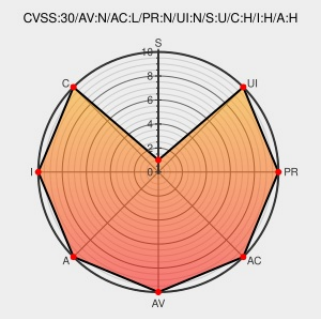
CVE-2015-1006

Published on: 05/10/2019 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:10 PM UTC

CVE-2015-1006

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



Certain versions of Optodatalink from Opto22 contain the following vulnerability:

A vulnerable file in Opto 22 PAC Project Professional versions prior to R9.4006, PAC Project Basic versions prior to R9.4006, PAC Display Basic versions prior to R9.4f, PAC Display Professional versions prior to R9.4f, OptoOPCServer versions prior to R9.4c, and OptoDataLink version R9.4d and prior versions that were installed by PAC Project installer, versions prior to R9.4006, is susceptible to a heap-based buffer overflow condition that may allow remote code execution on the target system. Opto 22 suggests upgrading to the new product version as soon as possible.

CVE-2015-1006 has been assigned by ics-cert@hq.dhs.gov to track the vulnerability - currently rated as CRITICAL severity.

CVSS3 Score: 9.8 - CRITICAL

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: 10 - HIGH

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

CVE References

Description	Tags	Link

OPTO 22 Multiple Product Vulnerabilities | ICS-CERT	Mitigation Third Party Advisory US Government Resource ics-cert.us-cert.gov text/html	MISC ics-cert.us-cert.gov/advisories/ICSA-15-120-01

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.

Related QID Numbers

590556 Opto 22 Multiple Product Multiple Vulnerabilities (ICSA-15-120-01)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Opto22	Optodatalink	All	All	All	All
Application	Opto22	Optodatalink	All	All	All	All
Application	Opto22	Optoopcserver	All	All	All	All
Application	Opto22	Optoopcserver	All	All	All	All
Application	Opto22	Pac Display	All	All	All	All
Application	Opto22	Pac Display	All	All	All	All
Application	Opto22	Pac Display	All	All	All	All
Application	Opto22	Pac Display	All	All	All	All
Application	Opto22	Pac Project	All	All	All	All
Application	Opto22	Pac Project	All	All	All	All
Application	Opto22	Pac Project	All	All	All	All
Application	Opto22	Pac Project	All	All	All	All

cpe:2.3:a:opto22:optodatalink:*:*:*:*:*:*:*:*:

cpe:2.3:a:opto22:optodatalink:*:*:*:*:*:*:*:*:

cpe:2.3:a:opto22:optoopcserver:*:*:*:*:*:*:*:*:

cpe:2.3:a:opto22:optoopcserver:*:*:*:*:*:*:*:*:

cpe:2.3:a:opto22:pac_display:*:*:*:*:basic:*:*:*:

cpe:2.3:a:opto22:pac_display:*:*:*:*:professional:*:*:*:

cpe:2.3:a:opto22:pac_display:*:*:*:*:basic:*:*:*:

cpe:2.3:a:opto22:pac_display:*:*:*:*:professional:*:*:*:

cpe:2.3:a:opto22:pac_project:*:*:*:*:basic:*:*:*:

cpe:2.3:a:opto22:pac_project:*:*:*:*:professional:*:*:*:

cpe:2.3:a:opto22:pac_project:*:*:*:*:basic:*:*:*:

cpe:2.3:a:opto22:pac_project:*:*:*:*:professional:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→