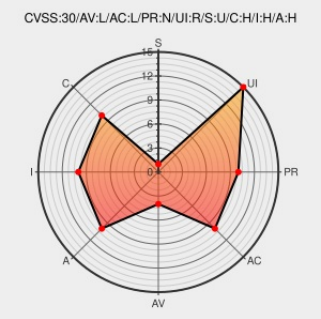
CVE-2015-1007

Published on: 03/25/2019 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:09 PM UTC

CVE-2015-1007

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



Certain versions of Optodatalink from Opto22 contain the following vulnerability:

A specially crafted configuration file could be used to cause a stack-based buffer overflow condition in the OPCTest.exe, which may allow remote code execution on Opto 22 PAC Project Professional versions prior to R9.4008, PAC Project Basic versions prior to R9.4008, PAC Display Basic versions prior to R9.4g, PAC Display Professional versions prior to R9.4g, OptoOPCServer version R9.4c and prior that were installed by PAC Project installer, versions prior to R9.4008, and OptoDataLink version R9.4d and prior that were installed by PAC Project installer, versions prior to R9.4008. Opto 22 suggests upgrading to the new product version as soon as possible.

CVE-2015-1007 has been assigned by ics-cert@hq.dhs.gov to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 7.8 - HIGH

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

CVSS2 Score: 9.3 - HIGH

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

CVE References

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

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	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: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→