CVE-2010-5333

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2010-5333
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-09-13 16:15:00 UTC
Updated	2019-09-24 17:15:00 UTC
Description	The web server in Integard Pro and Home before 2.0.0.9037 and 2.2.x before 2.2.0.9037 has a buffer overflow via a long pa

Risk And Classification

Problem Types: CWE-120

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Integard Home Project	Integard Home	All	All	All	All
Application	Integard Home Project	Integard Home	All	All	All	All
Application	Integard Pro Project	Integard Pro	All	All	All	All
Application	Integard Pro Project	Integard Pro	All	All	All	All

References

Reference	Source	Link	Tags
Integard Home and Pro v2 Remote HTTP Buffer Overflow Exploit	MISC	www.exploit-db.com	Explo
Integard Pro 2.2.0.9026 (Win7 ROP-Code Metasploit Module)	MISC	www.exploit-db.com	Explo
OSCE-prep/eip_integard.py at master · purpl3-f0x/OSCE-prep · GitHub	MISC	github.com	
purpl3f0xsec.tech - purpl3f0xsec Resources and Information.	MISC	purpl3f0xsec.tech	
metasploit-framework/integard_password_bof.rb at master · rapid7/metasploit-framework · GitHub	MISC	github.com	Explo
CVE Program record	CVE.ORG	www.cve.org	canor
NVD vulnerability detail	NVD	nvd.nist.gov	canor

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

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