



CVE-2012-1812

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2012-1812
State	PUBLIC
Assigner	cert@cert.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2012-11-13 13:39:00 UTC
Updated	2017-08-29 01:31:00 UTC
Description	eosfailoverservice.exe in C3-ilex EOscada before 11.0.19.2 allows remote attackers to obtain sensitive cleartext information

Risk And Classification

Problem Types: CWE-200

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	C3-ilex	Eoscada	All	All	All	All

References

Reference	Source	Link
C3-ilex EOscada Multiple Security Vulnerabilities	BID	www.securityfocus.com/bid/57844
C3-ilex EOscada Multiple Vulnerabilities ICS-CERT	MISC	www.us-cert.gov/ics/cert/alerts/ics-cert-12-024
IBM X-Force Exchange	XF	exchange.xforce.ibmcloud.com/vulnerabilities/57844
Security Advisory SA51171 - EOscada Information Disclosure and Denial of Service Vulnerabilities - Secunia	SECUNIA	secunia.com/advisories/51171
CVE Program record	CVE.ORG	www.cve.org/CVE/nvd/cve/2012/1812
NVD vulnerability detail	NVD	nvd.nist.gov/vuln/detail/CVE-2012-1812

No vendor comments have been submitted for this CVE.

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

this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

Free CVE JSON API cve.report/api

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