



CVE-2016-6890

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

Summary

CVE	CVE-2016-6890
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-01-05 22:59:00 UTC
Updated	2017-01-06 15:14:00 UTC
Description	Heap-based buffer overflow in MatrixSSL before 3.8.6 allows remote attackers to execute arbitrary code via a crafted Subject

Risk And Classification

Problem Types: CWE-119

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Matrixssl	Matrixssl	All	All	All	All

References

Reference	Source	Link	Tags
MatrixSSL VU#396440 Heap Based Buffer Overflow and Multiple Denial of Service Vulnerabilities	BID	www.securityfocus.com	Threat
matrixssl/CHANGES.md at 3-8-6-open · matrixssl/matrixssl · GitHub	CONFIRM	github.com	Package
Flawed MatrixSSL Code Highlights Need for Better IoT Update Practices	MISC	www.tripwire.com	Technical
Vulnerability Note VU#396440 - MatrixSSL contains multiple vulnerabilities	CERT-VN	www.kb.cert.org	Threat
CVE Program record	CVE.ORG	www.cve.org	Category
NVD vulnerability detail	NVD	nvd.nist.gov	Category

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](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)