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 Subje

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

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