



CVE-2017-2206

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

Summary

CVE	CVE-2017-2206
State	PUBLIC
Assigner	vultures@jpcert.or.jp
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-06-09 16:29:00 UTC
Updated	2017-06-20 15:14:00 UTC
Description	Untrusted search path vulnerability in the installer of SaAT Netizen ver.1.2.10.510 and earlier allows an attacker to gain priv

Risk And Classification

Problem Types: CWE-426

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Saat	Netizen	1.2.10.510	All	All	All
Application	Saat	Netizen	1.2.10.510	All	All	All

References

Reference
SaAT Netizen セキュリティアップデートのお知らせ インフォメーション SaAT サート セキュリティサービス Security & Assistant Tools
SaAT Netizen CVE-2017-2206 DLL Loading Remote Code Execution Vulnerability
JVN#91170929: Installer of SaAT Netizen may insecurely load Dynamic Link Libraries
CVE Program record
NVD vulnerability detail

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