



CVE-2017-14680

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

Summary

CVE	CVE-2017-14680
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-09-21 23:29:00 UTC
Updated	2017-10-03 17:03:00 UTC
Description	ZKTeco ZKTime Web 2.0.1.12280 allows remote attackers to obtain sensitive employee metadata via a direct request for a

Risk And Classification

Problem Types: CWE-200

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Zkteco	Zktime Web	2.0.1.12280	All	All	All
Application	Zkteco	Zktime Web	2.0.1.12280	All	All	All

References

Reference	Source	Link	Tags
Bugtraq: ZK Time_Web Software 2.0 - Broken Authentication	MISC	seclists.org	Exploit, Mailing List, Third Party Advisory
Full Disclosure: ZK Time_Web Software 2.0 - Broken Authentication	MISC	seclists.org	Exploit, Mailing List, Third Party Advisory
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

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

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