CVE-2017-13083

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2017-13083
State	PUBLISHED
Assigner	certcc
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-10-18 13:29:00 UTC
Updated	2026-04-07 13:07:23 UTC
Description	Akeo Consulting Rufus prior to version 2.17.1187 does not adequately validate the integrity of updates downloaded over HT

Risk And Classification

Primary CVSS: v3.0 8.1 HIGH from nvd@nist.gov

CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H

EPSS: 0.001140000 probability, percentile 0.299470000 (date 2026-04-07)

Problem Types: CWE-295 | CWE-345 | CWE-347 | CWE-494 | CWE-295 CWE-295: Improper Certificate Validation | CWE-494 CWE-494: Download of Code Without Integrity Check | CWE-345 CWE-345: Insufficient Verification of Data Authenticity | CWE-347 CWE-347: Improper Verification of Cryptographic Signature

Version	Source	Type	Score	Severity	Vector
3.0	nvd@nist.gov	Primary	8.1	HIGH	CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H
3.0	cret@cert.org	Secondary	5.3	MEDIUM	CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:N/I:H/A:N
3.0	CNA	DECLARED	5.3	MEDIUM	CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:N/I:H/A:N
2.0	nvd@nist.gov	Primary	6.8		AV:N/AC:M/Au:N/C:P/I:P/A:P

CVSS v3.0 Breakdown

Attack Vector

Network

Attack Complexity

High

Privileges Required

None

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Medium

Authentication

None

Confidentiality

Partial

Integrity

Partial

Availability

Partial

AV:N/AC:M/Au:N/C:P/I:P/A:P

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Akeo	Rufus	All	b1186	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Akeo Consulting	Rufus	affected prior to 2.17.1187	Not specified

References

Reference	Source
Vulnerability Note VU#403768 - Akeo Consulting Rufus fails to update itself securely	af854a3a-212
Akeo Consulting Rufus CVE-2017-13083 Arbitrary Code Execution Vulnerability	af854a3a-212
ER: Avoid prompts that users may not properly intepret on update signature validation · Issue #1009 · pbatard/rufus · GitHub	af854a3a-212
[pki] fix https://www.kb.cert.org/vuls/id/403768 · pbatard/rufus@c3c39f7 · GitHub	af854a3a-212

CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

Vendor Comments And Credit

Discovery Credit

CNA: Reported by Will Dormann of the CERT/CC (en)

Additional Advisory Data

Workarounds

CNA: Manually download updates from https://rufus.akeo.ie/

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