



Detect-It-Easy < 3.21 Path Traversal Arbitrary File Write

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

Summary

CVE	CVE-2026-43616
State	PUBLISHED
Assigner	VulnCheck
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-05-04 18:16:32 UTC
Updated	2026-05-04 18:16:32 UTC
Description	Detect-It-Easy prior to 3.21 contains a path traversal vulnerability that allows attackers to write arbitrary files to the filesystem

Risk And Classification

Primary CVSS: v4.0 6.8 MEDIUM from disclosure@vulncheck.com

CVSS:4.0/AV:L/AC:L/AT:N/PR:N/UI:A/VC:N/VI:H/VA:H/SC:N/SI:N/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

Problem Types: CWE-23 | CWE-23 CWE-23: Relative Path Traversal

Version	Source	Type	Score	Severity	Vector
4.0	disclosure@vulncheck.com	Secondary	6.8	MEDIUM	CVSS:4.0/AV:L/AC:L/AT:N/PR:N/UI:A/VC:N/VI:H/VA:H/SC:N/SI:N/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X
4.0	CNA	CVSS	6.8	MEDIUM	CVSS:4.0/AV:L/AC:L/AT:N/PR:N/UI:A/VC:N/VI:H/VA:H/SC:N/SI:N/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X
3.1	disclosure@vulncheck.com	Primary	7.1	HIGH	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:N/I:H/A:H
3.1	CNA	CVSS	7.1	HIGH	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:N/I:H/A:H

CVSS v4.0 Breakdown

Attack Vector

Local

Attack Complexity

Low

Attack Requirements

None

Privileges Required

None

User Interaction

Active

Active

Confidentiality

None

Integrity

High

Availability

High

Sub Conf.

None

Sub Integrity

None

Sub Availability

None

CVSS:4.0/AV:L/AC:L/AT:N/PR:N/UI:A/VC:N/VI:H/VA:H/SC:N/SI:N/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSX/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

CVSS v3.1 Breakdown

Attack Vector

Local

Attack Complexity

Low

Privileges Required

None

User Interaction

Required

Scope

Unchanged

Confidentiality

None

Integrity

High

Availability

High

CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:N/I:H/A:H

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Horsicq	DIE-engine	affected 3.21.0 semver	Not specified

References

Reference	Source	Link
aithub.com/horsica/XArchive/commit/6a2aa84c2fd120b704f76bb5c5ee3e9b5a7a0fcc	disclosure@vulncheck.com	aithub.com

github.com/horsicq/Format/commit/56cdf50ee3c72c56284e2819b23e98332842d259	disclosure@vulncheck.com	github.com
www.vulncheck.com/advisories/detect-it-easy-path-traversal-arbitrary-file-write	disclosure@vulncheck.com	www.vulncheck.com
github.com/horsicq/DIE-engine/commit/cbbe1688e58ffd430d284bf65f336973f08...	disclosure@vulncheck.com	github.com
github.com/horsicq/DIE-engine/commit/7fd300b926daf19707b2a36f0abe8b60a51...	disclosure@vulncheck.com	github.com
github.com/horsicq/Detect-It-Easy	disclosure@vulncheck.com	github.com
github.com/horsicq/Format/commit/56cdf50ee3c72c56284e2819b23e98332842d259	disclosure@vulncheck.com	github.com
github.com/horsicq/DIE-engine/releases/tag/3.21	disclosure@vulncheck.com	github.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

Vendor Comments And Credit

Discovery Credit
CNA: Mobasi Security Team (en)

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

© CVE.report 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to 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