



CVE-2007-2457

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

Summary

CVE	CVE-2007-2457
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2007-05-02 18:19:00 UTC
Updated	2026-04-23 00:35:47 UTC
Description	PHP remote file inclusion vulnerability in resources/includes/class.Smarty.php in Pixaria Gallery before 1.4.3 allows remote

Risk And Classification

Primary CVSS: v2.0 7.5 from nvd@nist.gov

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

Problem Types: NVD-CWE-Other | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

Partial

Integrity

Partial

Availability

Partial

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Pixaria	Pixaria Gallery	1.0.1	All	All	All

Application	Pixaria	Pixaria Gallery	1.0.2	All	All	All
Application	Pixaria	Pixaria Gallery	1.0.3	All	All	All
Application	Pixaria	Pixaria Gallery	1.0.4	All	All	All
Application	Pixaria	Pixaria Gallery	1.0.5	All	All	All
Application	Pixaria	Pixaria Gallery	1.1	All	All	All
Application	Pixaria	Pixaria Gallery	1.1.1	All	All	All
Application	Pixaria	Pixaria Gallery	1.1.2	All	All	All
Application	Pixaria	Pixaria Gallery	1.1.3	All	All	All
Application	Pixaria	Pixaria Gallery	1.1.4	All	All	All
Application	Pixaria	Pixaria Gallery	1.1.5	All	All	All
Application	Pixaria	Pixaria Gallery	1.1.6	All	All	All
Application	Pixaria	Pixaria Gallery	1.2	All	All	All
Application	Pixaria	Pixaria Gallery	1.2.1	All	All	All
Application	Pixaria	Pixaria Gallery	1.3	All	All	All
Application	Pixaria	Pixaria Gallery	1.3.1	All	All	All
Application	Pixaria	Pixaria Gallery	1.3.2	All	All	All
Application	Pixaria	Pixaria Gallery	1.3.3	All	All	All
Application	Pixaria	Pixaria Gallery	1.4	All	All	All
Application	Pixaria	Pixaria Gallery	1.4.1	All	All	All
Application	Pixaria	Pixaria Gallery	1.4.2	All	All	All

Vendor Declared Affected Products						
Source	Vendor	Product	Version	Platforms		
CNA	Na	N/a	affected n/a	Not specified		

References						
Reference			Source		Link	
Pixaria Gallery Class.SmartypHP Remote File Include Vulnerability			af854a3a-2127-422b-91ae-364da2661108		www.securityfocus.com	
IBM X-Force Exchange			af854a3a-2127-422b-91ae-364da2661108		exchange.xforce.ibm	
Pixaria Gallery 1.x (class.SmartypHP) Remote File Include Vulnerability			af854a3a-2127-422b-91ae-364da2661108		www.exploit-db.com	
Pixaria Gallery "cfg[sys][base_path]" File Inclusion - Advisories - Secunia			af854a3a-2127-422b-91ae-364da2661108		secunia.com	
SecurityFocus			af854a3a-2127-422b-91ae-364da2661108		www.securityfocus.com	
osvdb.org/34976			af854a3a-2127-422b-91ae-364da2661108		osvdb.org	
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH			af854a3a-2127-422b-91ae-364da2661108		www.vupen.com	
Pixaria 2 Version History			af854a3a-2127-422b-91ae-364da2661108		pixaria.com	
Pixaria 2 Latest News			af854a3a-2127-422b-91ae-364da2661108		www.pixaria.com	
Pixaria 2 Latest News			af854a3a-2127-422b-91ae-364da2661108		www.pixaria.com	

PIXARIA 2 Latest news	a1634a3a-2127-422b-91ae-3b40a2b61106	www.pixaria.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov
No vendor comments have been submitted for this CVE.		
There are currently no legacy QID mappings associated with this CVE.		

© [CVE.report](https://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](https://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.mitre.org/cve). This site includes MITRE data granted under the following [license](https://www.mitre.org/cve).

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report