



CVE-2002-1867

Published on: 12/31/2002 05:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:02 PM UTC

CVE-2002-1867

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Imagefolio](#) from [Bizdesign](#) contain the following vulnerability:

The default configuration of BizDesign ImageFolio 2.23 through 2.26 does not control access to (1) admin/setup.cgi, which allows remote attackers to create an administrative account, or (2) admin/nph-build.cgi, which allows remote attackers to cause a denial of service (CPU consumption).

CVE-2002-1867 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **7.5 - HIGH**

**Access
Vector**

NETWORK

**Access
Complexity**

LOW

Authentication

NONE

**Confidentiality
Impact**

PARTIAL

**Integrity
Impact**

PARTIAL

**Availability
Impact**

PARTIAL

CVE References

Description

Tags

Link

BizDesign ImageFolio setup.cgi Unauthorized User Creation Vulnerability

[cve.report \(archive\)](#)
[text/html](#)

[🌐](#) [BID 4975](#)

'[LoWNOISE] ImageFolio Pro 2.2' - MARC

[marc.info](#)
[text/html](#)

[🌐](#) [BUGTRAQ 20020609](#)
[\[LoWNOISE\] ImageFolio Pro 2.2](#)

ISS X-Force Database: imagefolio-setup-cgi-access (9308): ImageFolio setup.cgi script can be accessed remotely

[web.archive.org](#)
[text/html](#)

[Inactive Link](#) [Not Archived](#)

[🌐](#) [XF imagefolio-setup-cgi-access\(9308\)](#)

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to

comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Bizdesign	Imagefolio	2.23	All	All	All
Application	Bizdesign	Imagefolio	2.24	All	All	All
Application	Bizdesign	Imagefolio	2.26	All	All	All
Application	Bizdesign	Imagefolio	2.23	All	All	All
Application	Bizdesign	Imagefolio	2.24	All	All	All
Application	Bizdesign	Imagefolio	2.26	All	All	All

cpe:2.3:a:bizdesign:imagefolio:2.23:*****:

cpe:2.3:a:bizdesign:imagefolio:2.24:*****:

cpe:2.3:a:bizdesign:imagefolio:2.26:*****:

cpe:2.3:a:bizdesign:imagefolio:2.23:*****:

cpe:2.3:a:bizdesign:imagefolio:2.24:*****:

cpe:2.3:a:bizdesign:imagefolio:2.26:*****:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→