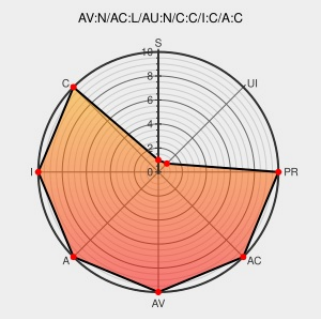
CVE-2004-1763

Published on: 12/31/2004 05:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:10 PM UTC

CVE-2004-1763

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Hahtsite Scenario Server from Haht Commerce contain the following vulnerability:

Buffer overflow in hsrun.exe for HAHTsite Scenario Server 5.1 Patch 06 (build 91) allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via a long project name.

CVE-2004-1763 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 10 - HIGH

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
HAHTsite Scenario Server Project File Name Buffer Overrun Vulnerability	Patch, cve.report (archive), text/html	BID 10033
IBM X-Force Exchange	exchange.xforce.ibmcloud.com, text/html	XF hahtsite-long-request-bo(15717)
No Description Provided	web.archive.org, text/html, Inactive Link, Not Archived	MISC www.protego.dk/advisories/200405.html
'[Full-Disclosure] Buffer Overflow in HAHTsite Scenario Server 5.1' - MARC	marc.info, text/html	FULLDISC 20040402 Buffer Overflow in HAHTsite Scenario Server 5.1
US-CERT Vulnerability Note VU#705958	Third Party Advisory, US Government Resource, www.kb.cert.org	CERT-VN VU#705958

	text/html	
Secunia - Advisories - HAHTsite Scenario Server Project Name Buffer Overflow Vulnerability	Exploit Patch web.archive.org text/html	SECUNIA 11288

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	Haht Commerce	Hahtsite Scenario Server	5.1	All	All	All
Application	Haht Commerce	Hahtsite Scenario Server	5.1_patch_1	All	All	All
Application	Haht Commerce	Hahtsite Scenario Server	5.1_patch_2	All	All	All
Application	Haht Commerce	Hahtsite Scenario Server	5.1_patch_3	All	All	All
Application	Haht Commerce	Hahtsite Scenario Server	5.1_patch_4	All	All	All
Application	Haht Commerce	Hahtsite Scenario Server	5.1_patch_5	All	All	All
Application	Haht Commerce	Hahtsite Scenario Server	5.1_patch_6	All	All	All
Application	Haht Commerce	Hahtsite Scenario Server	5.1	All	All	All
Application	Haht Commerce	Hahtsite Scenario Server	5.1_patch_1	All	All	All
Application	Haht Commerce	Hahtsite Scenario Server	5.1_patch_2	All	All	All
Application	Haht Commerce	Hahtsite Scenario Server	5.1_patch_3	All	All	All
Application	Haht Commerce	Hahtsite Scenario Server	5.1_patch_4	All	All	All
Application	Haht Commerce	Hahtsite Scenario Server	5.1_patch_5	All	All	All
Application	Haht Commerce	Hahtsite Scenario Server	5.1_patch_6	All	All	All

cpe:2.3:a:haht_commerce:hahtsite_scenario_server:5.1:*:*:*:*:*:*:*:

cpe:2.3:a:haht_commerce:hahtsite_scenario_server:5.1_patch_1:*:*:*:*:*:*:*:

cpe:2.3:a:haht_commerce:hahtsite_scenario_server:5.1_patch_2:*:*:*:*:*:*:*:

cpe:2.3:a:haht_commerce:hahtsite_scenario_server:5.1_patch_3:*:*:*:*:*:*:*:

cpe:2.3:a:haht_commerce:hahtsite_scenario_server:5.1_patch_4:*:*:*:*:*:*:*:

cpe:2.3:a:haht_commerce:hahtsite_scenario_server:5.1_patch_5:*:*:*:*:*:*:*:

cpe:2.3:a:haht_commerce:hahtsite_scenario_server:5.1_patch_6:*:*:*:*:*:*:*:

cpe:2.3:a:haht_commerce:hahtsite_scenario_server:5.1:*:*:*:*:*:*:*:

cpe:2.3:a:haht_commerce:hahtsite_scenario_server:5.1_patch_1:*:*:*:*:*:*:*

cpe:2.3:a:haht_commerce:hahtsite_scenario_server:5.1_patch_2:*:*:*:*:*:*:*

cpe:2.3:a:haht_commerce:hahtsite_scenario_server:5.1_patch_3:*:*:*:*:*:*:*

cpe:2.3:a:haht_commerce:hahtsite_scenario_server:5.1_patch_4:*:*:*:*:*:*:*

cpe:2.3:a:haht_commerce:hahtsite_scenario_server:5.1_patch_5:*:*:*:*:*:*:*

cpe:2.3:a:haht_commerce:hahtsite_scenario_server:5.1_patch_6:*:*:*:*:*:*:*

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→