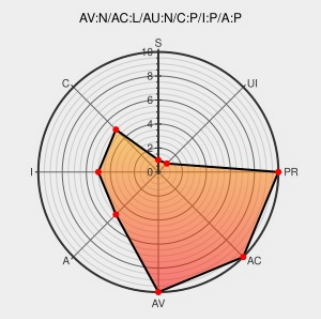
CVE-2004-1793

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

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

CVE-2004-1793

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



Certain versions of Switch Off from Yatsoft contain the following vulnerability:

Stack-based buffer overflow in swnet.dll in YaSoft Switch Off 2.3 and earlier allows remote authenticated users to execute arbitrary code via a long message parameter in a SendMsg action to action.htm.

CVE-2004-1793 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 7.5 - HIGH

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

CVE References

Description	Tags	Link
YaSoft Switch Off swnet.dll Remote Buffer Overflow Vulnerability	Exploit, cve.report (archive), text/html	BID 9340
	Exploit, www.elitehaven.net, text/plain, Inactive Link, Not Archived	MISC www.elitehaven.net/switchoff.txt
No Description Provided	www.osvdb.org, Inactive Link, Not Archived	OSVDB 3309
IBM X-Force Exchange	exchange.xforce.ibmcloud.com, text/html	XF switch-off-swnet-bo(14124)
Y@Soft Switch Off Lets Remote Users Deny Service and Remote	Exploit	SECTRACK 1008581

Authenticated Users Execute Arbitrary Code - SecurityTracker	securitytracker.com text/html	
Switch Off HTTP Request Handling Vulnerabilities - Advisories - Secunia	Exploit web.archive.org text/html	SECUNIA 10521
SecurityFocus	Exploit www.securityfocus.com text/html	BUGTRAQ 20040102 Switch Off Multiple Vulnerabilities

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	Yatsoft	Switch Off	0.7	All	All	All
Application	Yatsoft	Switch Off	1.0	All	All	All
Application	Yatsoft	Switch Off	1.1	All	All	All
Application	Yatsoft	Switch Off	1.2	All	All	All
Application	Yatsoft	Switch Off	1.3	All	All	All
Application	Yatsoft	Switch Off	1.4	All	All	All
Application	Yatsoft	Switch Off	1.5	All	All	All
Application	Yatsoft	Switch Off	1.5.1	All	All	All
Application	Yatsoft	Switch Off	1.6	All	All	All
Application	Yatsoft	Switch Off	1.7	All	All	All
Application	Yatsoft	Switch Off	1.8	All	All	All
Application	Yatsoft	Switch Off	1.9	All	All	All
Application	Yatsoft	Switch Off	2.0	All	All	All
Application	Yatsoft	Switch Off	2.1	All	All	All
Application	Yatsoft	Switch Off	2.2	All	All	All
Application	Yatsoft	Switch Off	2.3	All	All	All
Application	Yatsoft	Switch Off	0.7	All	All	All
Application	Yatsoft	Switch Off	1.0	All	All	All
Application	Yatsoft	Switch Off	1.1	All	All	All
Application	Yatsoft	Switch Off	1.2	All	All	All
Application	Yatsoft	Switch Off	1.3	All	All	All
Application	Yatsoft	Switch Off	1.4	All	All	All

Application	Yatsoft	Switch Off	1.5	All	All	All
Application	Yatsoft	Switch Off	1.5.1	All	All	All
Application	Yatsoft	Switch Off	1.6	All	All	All
Application	Yatsoft	Switch Off	1.7	All	All	All
Application	Yatsoft	Switch Off	1.8	All	All	All
Application	Yatsoft	Switch Off	1.9	All	All	All
Application	Yatsoft	Switch Off	2.0	All	All	All
Application	Yatsoft	Switch Off	2.1	All	All	All
Application	Yatsoft	Switch Off	2.2	All	All	All
Application	Yatsoft	Switch Off	2.3	All	All	All

cpe:2.3:a:yatsoft:switch_off:0.7:*:*:*:*:*:*:*:

cpe:2.3:a:yatsoft:switch_off:1.0:*:*:*:*:*:*:*:

cpe:2.3:a:yatsoft:switch_off:1.1:*:*:*:*:*:*:*:

cpe:2.3:a:yatsoft:switch_off:1.2:*:*:*:*:*:*:*:

cpe:2.3:a:yatsoft:switch_off:1.3:*:*:*:*:*:*:*:

cpe:2.3:a:yatsoft:switch_off:1.4:*:*:*:*:*:*:*:

cpe:2.3:a:yatsoft:switch_off:1.5:*:*:*:*:*:*:*:

cpe:2.3:a:yatsoft:switch_off:1.5.1:*:*:*:*:*:*:*:

cpe:2.3:a:yatsoft:switch_off:1.6:*:*:*:*:*:*:*:

cpe:2.3:a:yatsoft:switch_off:1.7:*:*:*:*:*:*:*:

cpe:2.3:a:yatsoft:switch_off:1.8:*:*:*:*:*:*:*:

cpe:2.3:a:yatsoft:switch_off:1.9:*:*:*:*:*:*:*:

cpe:2.3:a:yatsoft:switch_off:2.0:*:*:*:*:*:*:*:

cpe:2.3:a:yatsoft:switch_off:2.1:*:*:*:*:*:*:*:

cpe:2.3:a:yatsoft:switch_off:2.2:*:*:*:*:*:*:*:

cpe:2.3:a:yatsoft:switch_off:2.3:*:*:*:*:*:*:*:

cpe:2.3:a:yatsoft:switch_off:0.7:*:*:*:*:*:*:*:

cpe:2.3:a:yatsoft:switch_off:1.0:*:*:*:*:*:*:*:

cpe:2.3:a:yatsoft:switch_off:1.1:*:*:*:*:*:*:*:

cpe:2.3:a:yatsoft:switch_off:1.2:*:*:*:*:*:*:*:

cpe:2.3:a:yatsoft:switch_off:1.3:*:*:*:*:*:*:*

cpe:2.3:a:yatsoft:switch_off:1.4:*:*:*:*:*:*:*

cpe:2.3:a:yatsoft:switch_off:1.5:*:*:*:*:*:*:*

cpe:2.3:a:yatsoft:switch_off:1.5.1:*:*:*:*:*:*:*

cpe:2.3:a:yatsoft:switch_off:1.6:*:*:*:*:*:*:*

cpe:2.3:a:yatsoft:switch_off:1.7:*:*:*:*:*:*:*

cpe:2.3:a:yatsoft:switch_off:1.8:*:*:*:*:*:*:*

cpe:2.3:a:yatsoft:switch_off:1.9:*:*:*:*:*:*:*

cpe:2.3:a:yatsoft:switch_off:2.0:*:*:*:*:*:*:*

cpe:2.3:a:yatsoft:switch_off:2.1:*:*:*:*:*:*:*

cpe:2.3:a:yatsoft:switch_off:2.2:*:*:*:*:*:*:*

cpe:2.3:a:yatsoft:switch_off:2.3:*:*:*:*:*:*:*

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→