

Search ..

Home Files News About Contact &[SERVICES\_TAB]

Add New

## FAUST iServer 9.0.018.018.4 Local File Inclusion

Authored by Mario Keck | Site sec-consult.com

Posted Jan 25, 2022

Land Software's FAUST iServer versions 9.0.017.017.1-3 through 9.0.018.018.4 suffer from a local file inclusion vulnerability.

tags | exploit, local, file inclusion

advisories | CVE-2021-34805 | SHA-256 | 1940c0374c57a3ce5c29fb1b1586c473fe48cd03993e507d365564b0b210c462 | Download | Favorite | View

Share This

LinkedIn Reddit Digg StumbleUpon



Su	Мо	Tu	We	Th	Fr
Sa					
				1	2
3					
4	5	6	7	8	9
10					
11	12	13	14	15	16
17					
18	19	20	21	22	23
24					
25	26	27	28	29	30
31					
			28		30

Top Aut	thors In Last 30 Days
Red Hat 1	57 files
Ubuntu 76	files
LiquidWo	rm 23 files
Debian 21	files
nu11secu	r1ty 11 files
malvuln 11	1 files
Gentoo 9 f	files
Google Se	ecurity Research 8 files
Julien Ahr	rens 4 files
T Weber 4	Lfiles

File Tags File Archives ActiveX (932) December 2022 Advisory (79,754) Arbitrary (15,694) October 2022 BBS (2.859) September 2022 Bypass (1,619) August 2022 July 2022 CGI (1,018) Code Execution (6,926) June 2022 Conference (673) May 2022 Cracker (840) April 2022 CSRF (3,290) March 2022 DoS (22.602) February 2022 Encryption (2,349) January 2022 Exploit (50,359) Older File Inclusion (4,165) File Upload (946) Systems Firewall (821) AIX (426) Info Disclosure (2,660) Apple (1,926) Intrusion Detection (867) BSD (370) Java (2,899) CentOS (55) JavaScript (821) Cisco (1.917) Kernel (6,291) Debian (6,634) Local (14,201) Magazine (586) FreeBSD (1.242) Gentoo (4,272) Perl (1.418) HPUX (878) PHP (5.093) iOS (330) Proof of Concept (2,291) iPhone (108) Protocol (3,435) IRIX (220) Python (1.467) Juniper (67) Remote (30.044) Linux (44,315) Root (3,504) Mac OS X (684) Ruby (594) Mandriva (3,105) Scanner (1.631) Security Tool (7,777) OpenBSD (479) Shell (3,103) RedHat (12.469) Shellcode (1,204) Slackware (941) Sniffer (886) Solaris (1,607)

Change Mirror						Download
SEC Consult Vulnerabil						
product: fixed version: fixed version: CVE number: impact: homepage: found: by:	9.0.019.019.7, Vers CVE-2021-34805	JST iServer 0.0.018.018.4 sion 10 oftware.de ermany) sbility Lab				
	Europe   Asia   Nor	th America	, an Acos con	aparry		
	https://www.sec-cor	nsult.com				
Vendor description: (German) "Der FAUST is ins Intranet und Inter Installation."	erver bringt Ihre F net. Er bietet hohe	FAUST- , FAUST E Sicherheit un	Entry- und L d eine einfa	IDOS-Datenban che	ken	
Source: http://www.lar	d-software.de/lfs.f	[au?prj=iweb&dn	=faust+iserv	er		
Business recommendation  The vendor provides a most actual version v1 the form of a patch is same partition as the	 hotfix for the ider 0 of FAUST iServer required. The webs	is not vulnera oot of the ser	ble, no immed ver should no	diate action	in	
Vulnerability overvies  1) Local File Inclusic When a URL is requeste file on the operating webserver pages for di vulnerable versions of aiming to read local f	n (CVE-2021-34805) d, the FAUST iServe system. ".fau" file splaying the conter FAUST iServer do r	es can be compa it of the webpa not properly pr	red with comp	oiled tified		
FAUST iServer is design Therefore, by simply U \\windows\win.i the FAUST iServer retu	RL-encoding a path ni into %2e%2e%5c%2	like 2e%2e%5c%2e%2e%				
Proof of concept:  1) Local File Inclusic The following proof of local files of the ser The vulnerability, as triggered as soon as a operating system speci on the same partition Authorization is not r	concept shows the ver's operating sys shown in the proof vulnerable version fic files, the webr as the operating sy	of concept req of FAUST iSer coot of FAUST i	uest below, over is in use	can be		
HTTP Request: GET /*\$5c\$2e\$2e\$5c\$2e\$2e\$5c*1 HTTP/1.1 User-Agent: Mozilla/5. Connection: Keep-alive Host: <tp>Accept: text/html, appl Accept-Language: en-US</tp>	0 (Windows NT 6.1;	WOW64; Trident	/7.0; rv:11.0	) like Gecko		c\$2e\$2e\$5c\$2e\$2e\$5
Vulnerable / tested versions The following versions * 9.0.017.017.1-3 * 9.0.018.018.4		and found to be	vulnerable:			
2021-06-15: Requested vulnerabl 2021-06-17: Vendor inf inform al 2021-08-09: Confirmed 2021-08-16: Researcher newslette 2022-01-12: Version 10	vendor via email. uested more informe ded on the same day information from ve e. ormed researcher at l customers about t the security fix ir received a notific r announcing the of was officially rel for upgrade.	endor to check cout upcoming us the critical set or FAUST iServer cation mail fro efficial release	which version update and pro- curity fix in 9.0.019.019 im the vendor	omised to n it. .7. 's		
Solution:  The vulnerability is f * 9.0.019.019.7	ixed in the followi	ing version:				
This patch should be in Version 10 is not affect to upgrade to this ver	cted by this vulner		essible it is	recommended		
Workeround:						
Advisory URL: https://sec-consult.co	m/vulnerability-lah	»/				

SEC Consult Vulnerability Lab Spoof (2,166) SUSE (1,444) SEC Consult, an Atos company Europe | Asia | North America SQL Injection (16,102) Ubuntu (8,199) About SEC Consult Vulnerability Lab
The SEC Consult Vulnerability Lab is an integrated part of SEC Consult, an
Akos company. It ensures the continued knowledge gain of SEC Consult in the
field of network and application security to stay ahead of the attacker. The
SEC Consult Vulnerability Lab supports high-quality penetration testing and
the evaluation of new offensive and defensive technologies for our customers.
Hence our customers obtain the most current information about vulnerabilities
and valid recommendation about the risk profile of new technologies. TCP (2,379) UNIX (9,159) UDP (876) Windows (6,511) Other Virus (662) Vulnerability (31,136) Web (9,365) Whitepaper (3,729) Interested in improving your cyber security with the experts of SEC Consult? Contact our local offices https://sec-consult.com/contact/ x86 (946) XSS (17,494) Other Mail: research at sec-consult dot com
Web: https://www.sec-consult.com
Blog: http://blog.sec-consult.com
Twitter: https://twitter.com/sec\_consult EOF Mario Keck / @2022 Login or Register to add favorites



## Site Links

News by Month

News Tags Files by Month

File Tags File Directory

## About Us

History & Purpose Contact Information

Terms of Service Privacy Statement

Copyright Information

## **Hosting By**

Follow us on Twitter

