Threat Analysis Reports

CVE-2022-0609: This vulnerability affects Google Chrome versions prior to 98.0.4758.102. This exploit exploits the animation functionality of a web page in chrome. Possible effects include running malicious code on the user's computer for first access or causing the application to crash. The possible attack scenario is as follows: A hacker exploits the code of a website. He manipulates the part of the code that contains the animation functions of the site. Here, when the user opens the web page, a malicious shellcode is embedded in the memory section where the code containing the animation functions is executed. In normal cases, the memory section in question is freed because the animation function is terminated, but due to this vulnerability on chrome, the memory section is released without being cleaned. The code manipulated by the hacker tries to reuse the freed memory section, which of course causes an error, but with this method, the malicious shellcode left in the memory section is executed.

Mitigation: Update Google chrome to the latest version. Use Firewalls and IDS/IPS Solutions. Monitor the entire environment for the use of credentials that were on system. Monitor network logs for signs of data exfiltration and lateral movement.

Source:

https://issues.chromium.org/issues/40058745

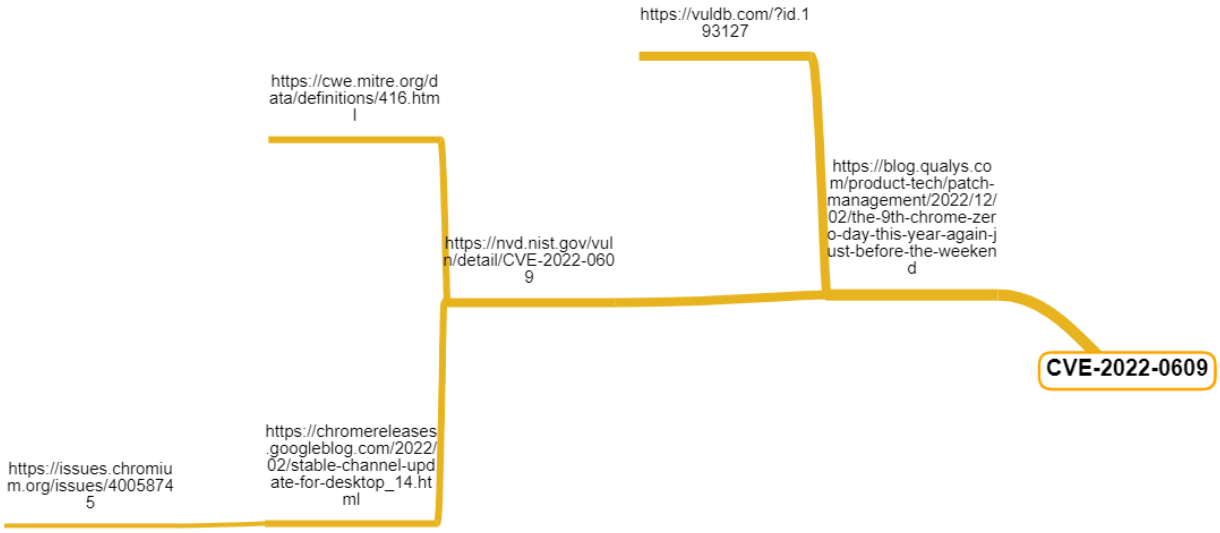
https://chromereleases.googleblog.com/2022/02/stable-channel-update-for-desktop_14.html

https://cwe.mitre.org/data/definitions/416.html

https://vuldb.com/?id.193127

https://nvd.nist.gov/vuln/detail/CVE-2022-0609

https://blog.qualys.com/product-tech/patch-management/2022/12/02/the-9th-chrome-zero-day-this-year-again-just-before-the-weekend



CVE-2023-2868: This vulnerability affects Barracuda Email Security Gateway products.

In this vulnerability, the attacker first creates a tar file that exploits this vulnerability, which typically contains 5 files, one of which contains a base64 encoded text enclosed in back quotes (`) and single quotes (') that triggers command injection in the form of command substitution. The other files are junk files containing random data. The attacker sends phishing emails from various servers, initially sending attached files with the .tar extension, later the extensions change, but ultimately it remains a tar file. When the victim tries to analyze the tar file, the poisoned file runs code in the background that will continue to run even if the command line is closed. This code first creates a folder with a storage point (such as /tmp/p), then connects to an ip address with openssl, and then deletes the storage it created to erase its traces. After gaining access to the system, the hacker opens backdoors in the system by installing multiple backdoor applications. The methods he applies to ensure his persistence in the system are self-execution through daily and hourly cron jobs for reverse shell. For backdoors, manipulating the /etc/init.d/rc file to automatically activate backdoors when the system starts. In the data theft phase, in the majority of cases, it stored data in .tar.gz files in the /mail/tmp/ directory and used a consistent file naming convention of 3 letters followed by a number, such as 001, corresponding to the victim organization. it then exfiltrated this data to its own system over an openssl connection. The most well-known group exploiting this vulnerability is UNC4841. Experts believe that this group is conducting espionage activities for the Republic of China.

Network IOCs

IP Address	ASN	Netblock	Location
101.229.146.218	4812	China Telecom	CN
103.146.179.101	136933	Gigabitbank Global	HK
103.27.108.62	132883	Topway Global Limited	HK
103.77.192.13	10222	Multibyte Info Technology Limited	HK
103.77.192.88	10222	Multibyte Info Technology Limited	HK
103.93.78.142	61414	Edgenap Ltd	JP
104.156.229.226	20473	Choopa, LLC	US
104.223.20.222	8100	CloudVPS	US
107.148.149.156	399195	Pegtechinc-ap-04	US
107.148.219.227	54600	Peg Tech	US
107.148.219.53	54600	Peg Tech	US
107.148.219.54	54600	Peg Tech	US
107.148.219.55	54600	Peg Tech	US
107.148.223.196	54600	Peg Tech	US
107.173.62.158	20278	Nexeon Technologies	US
137.175.19.25	54600	Peg Tech	US
137.175.28.251	54600	Peg Tech	US
137.175.30.36	54600	Peg Tech	US
137.175.30.86	54600	Peg Tech	US
137.175.51.147	54600	Peg Tech	US
137.175.53.17	54600	Peg Tech	US
137.175.53.170	54600	Peg Tech	US
137.175.53.218	54600	Peg Tech	US
137.175.60.252	54600	Peg Tech	US
137.175.60.253	54600	Peg Tech	US
137.175.78.66	54600	Peg Tech	US
139.84.227.9	20473	Choopa, LLC	ZA
155.94.160.72	8100	CloudVPS	US
182.239.114.135	9231	China Mobile Hong Kong	HK
182.239.114.254	9231	China Mobile Hong Kong	HK
192.74.226.142	54600	Peg Tech	CN
192.74.254.229	54600	Peg Tech	US
198.2.254.219	54600	Peg Tech	US
198.2.254.220	54600	Peg Tech	US
198.2.254.221	54600	Peg Tech	US
198.2.254.222	54600	Peg Tech	US
198.2.254.223	54600	Peg Tech	US
199.247.23.80	20473	Choopa, LLC	DE

213.156.153.34	202422	G-Core Labs S.A.	US
216.238.112.82	20473	Choopa, LLC	BR
23.224.42.29	40065	Cnservers LLC	US
23.224.78.130	40065	Cnservers LLC	US
23.224.78.131	40065	Cnservers LLC	US
23.224.78.132	40065	Cnservers LLC	US
23.224.78.133	40065	Cnservers LLC	US
23.224.78.134	40065	Cnservers LLC	US
37.9.35.217	202422	G-Core Labs S.A.	US
38.54.113.205	138915	Kaopu Cloud HK Limited	MY
38.54.1.82	138915	Kaopu Cloud HK Limited	SG
38.60.254.165	174	Cogent Communications	US
45.63.76.67	20473	Choopa, LLC	US
52.23.241.105	14618	Amazon.com	US
64.176.4.234	20473	Choopa, LLC	US
64.176.7.59	20473	Choopa, LLC	US

Domain
bestfindthetruth[.]com
fessionalwork[.]com
gesturefavour[.]com
goldenunder[.]com
singamofing[.]com
singnode[.]com
togetheroffway[.]com
troublendsef[.]com

Endpoint IOCs

Hash	Filename	Type
0d67f50a0bf7a3a017784146ac41ada0	snapshot.tar	Payload Attachment
42722b7d04f58dcb8bd80fe41c7ea09e	11111.tar	Payload Attachment
5392fb400bd671d4b185fb35a9b23fd3	imgdata.jpg	Payload Attachment
ac4fb6d0bfc871be6f68bfa647fc0125	snapshot.tar	Payload Attachment
878cf1de91f3ae543fd290c31adcbda4	snapshot.tar	Payload Attachment
b601fce4181b275954e3f35b18996c92	install_reuse.tar	SALTWATER install
827d507aa3bde0ef903ca5dec60cdec8	mod_udp.so	SALTWATER variant
c56d7b86e59c5c737ee7537d7cf13df1	autoins	SALTWATER install
6f79ef58b354fd33824c96625590c244	intent_reuse	SALTWATER install
349ca242bc6d2652d84146f5f91c3dbb	intentbas	SALTWATER install
1fea55b7c9d13d822a64b2370d015da7	mod_udp.so	SALTWATER variant
64c690f175a2d2fe38d3d7c0d0ddbb6e	mod_udp.so	SALTWATER variant
4cd0f3219e98ac2e9021b06af70ed643	mod_udp.so	SALTWATER variant
3b93b524db66f8bb3df8279a141734bb	mod_rtf.so	SALTWATER variant
8fdf3b7dc6d88594b8b5173c1aa2bc82	mod_rft.so	SALTWATER Variant
4ec4ceda84c580054f191caa09916c68	mod_rft.so	SALTWATER variant
1b1830abaf95bd5a44aa3873df901f28	mod_rft.so	SALTWATER variant
4ca4f582418b2cc0626700511a6315c0	BarracudaMailService	SEASPY Variant

c528b6398c86f8bdcfa3f9de7837ebfe	update_v2.sh	SEASPY Install
2d841cb153bebcfdee5c54472b017af2	rc	SEASPY launcher
c979e8651c1f40d685be2f66e8c2c610	rc	SEASPY launcher
1c042d39ca093b0e7f1412453b132076	rc	SEASPY launcher
ba7af4f98d85e5847c08cf6cefdf35dc	rc	SEASPY launcher
82eaf69de710abdc5dea7cd5cb56cf04	BarracudaMailService	SEASPY Variant
e80a85250263d58cc1a1dc39d6cf3942	BarracudaMailService	SEASPY Variant
5d6cba7909980a7b424b133fbac634ac	BarracudaMailService	SEASPY Variant
1bbb32610599d70397adfdaf56109ff3	BarracudaMailService	SEASPY Variant
4b511567cfa8dbaa32e11baf3268f074	BarracudaMailService	SEASPY Variant
a08a99e5224e1baf569fda816c991045	BarracudaMailService	SEASPY Variant
19ebfe05040a8508467f9415c8378f32	BarracudaMailService	SEASPY Variant
831d41ba2a0036540536c2f884d089f9	sendscd	SEASPY Variant
db4c48921537d67635bb210a9cb5bb52	BarracudaMailService	SEASPY Variant
694cdb49879f1321abb4605adf634935	install_bvp74_auth.tar	SEASPY install
5fdee67c82f5480edfa54afc5a9dc834	install_bvp74_auth.tar	SEASPY install
8fc03800c1179a18fbd58d746596fa7d	update_version	SEASPY launcher
17696a438387248a12cc911fbae8620e	resize_risertab	SEASPY launcher
4c1c2db989e0e881232c7748593d291e	update_version	SEASPY launcher
3e3f72f99062255d6320d5e686f0e212	update_version	SEASPY launcher
7d7fd05b262342a9e8237ce14ec41c3b	update_version	SEASPY launcher
2e30520f8536a27dd59eabbcb8e3532a	update_version	SEASPY launcher
0245e7f9105253ecb30de301842e28e4	update_version	SEASPY launcher
0c227990210e7e9d704c165abd76ebe2	update_version	SEASPY launcher
c7a89a215e74104682880def469d4758	update_version	SEASPY launcher
1bc5212a856f028747c062b66c3a722a	update_version	SEASPY launcher
a45ca19435c2976a29300128dc410fd4	update_version	SEASPY launcher
132a342273cd469a34938044e8f62482	update_version	SEASPY launcher
23f4f604f1a05c4abf2ac02f976b746b	resize2fstab	SEASPY Variant
45b79949276c9cb9cf5dc72597dc1006	resize_reisertab	SEASPY Variant
bef722484288e24258dd33922b1a7148	resize2fstab	SEASPY Variant
0805b523120cc2da3f71e5606255d29c	resize_reisertab	SEASPY Variant
69ef9a9e8d0506d957248e983d22b0d5	resize2fstab	SEASPY Variant
3c20617f089fe5cc9ba12c43c6c072f5	resize2fstab	SEASPY Variant
76811232ede58de2faf6aca8395f8427	resize2fstab	SEASPY Variant
f6857841a255b3b4e4eded7a66438696	resize_reisertab	SEASPY Variant
2ccb9759800154de817bf779a52d48f8	install_helo.tar	SEASIDE Install
cd2813f0260d63ad5adf0446253c2172	mod_require_helo.lua	SEASIDE variant
177add288b289d43236d2dba33e65956	rverify	WHIRLPOOL VARIANT
87847445f9524671022d70f2a812728f	mod_content.lua	SKIPJACK

35cf6faf442d325961935f660e2ab5a0	mod_attachment.lua	SEASPRAY
ce67bb99bc1e26f6cb1f968bc1b1ec21	install_att_v2.tar	SEASPRAY install
e4e86c273a2b67a605f5d4686783e0cc	mknod	SKIPJACK Persistence
ad1dc51a66201689d442499f70b78dea	get_fs_info.pl	SKIPJACK Persistence
9033dc5bac76542b9b752064a56c6ee4	nfsd_stub.ko	SANDBAR
e52871d82de01b7e7f134c776703f696	rverify	WHIRLPOOL Variant
446f3d71591afa37bbd604e2e400ae8b	mknod	SEASPRAY Persistence
666da297066a2596cacb13b3da9572bf	mod_sender.lua	SEASPRAY
436587bad5e061a7e594f9971d89c468	saslautchd	WHIRLPOOL Variant
85c5b6c408e4bdb87da6764a75008adf	rverify	WHIRLPOOL Variant
407738e565b4e9dafb07b782ebcf46b0	test1.sh	Reverse shell cronjob
cb0f7f216e8965f40a724bc15db7510b	update_v35.sh	Bash Script
N/A – multiple version identified	1.sh	Bash Script
19e373b13297de1783cecf856dc48eb0	cl	proxy client
N/A	aacore.sh	reverse shell cronjob
N/A	appcheck.sh	reverse shell cronjob
881b7846f8384c12c7481b23011d8e45	update_v31.sh	Bash Script
f5ab04a920302931a8bd063f27b745cc	intent_helo	Bash Script
N/A	p	Named pipe used in reverse shell
N/A	p7	Named pipe used in reverse shell
N/A	t	Named pipe used in reverse shell
N/A	core.sh	Reverse shell cronjob
N/A	p1	Named pipe used in reverse shell
177add288b289d43236d2dba33e65956	pd	WHIRLPOOL Variant
N/A	b	Named pipe used in reverse shell
d098fe9674b6b4cb540699c5eb452cb5	test.sh	Reverse shell cronjob
N/A	ss	Named pipe used in reverse shell

Mitigation: Sweep the impacted environment for all IOCs provided by both Mandiant and Barracuda. Review email logs to identify the initial point of exposure. Revoke and rotate all domain-based and local credentials that were

on the ESG at the time of compromise. Revoke and reissue all certificates that were on the ESG at the time of compromise. Monitor the entire environment for the use of credentials that were on the ESG at time of compromise. Review network logs for signs of data exfiltration and lateral movement.

Source:

https://www.vectra.ai/blog/technical-analysis-barracuda-email-security-gateway

https://status.barracuda.com/incidents/34kx82j5n4q9

https://www.mandiant.com/resources/blog/barracuda-esg-exploited-globally

https://nvd.nist.gov/vuln/detail/CVE-2023-2868

https://thehackernews.com/2023/05/barracuda-warns-of-zero-day-exploited.html

https://www.barracuda.com/company/legal/esg-vulnerability