Broadvoice database of more than 350 million customer records exposed online

By Paul Bischoff

Published: 2020-10-15 · Archived: 2026-04-05 14:33:20 UTC

A Broadvoice database cluster holding more than 350 million records, many including personal details and voicemail transcripts of Broadvoice clients' customers, was left open online for anyone to view with no authentication required for access, as discovered by Comparitech researchers.

Security expert Bob Diachenko, working on behalf of Comparitech, uncovered the database information on October 1. He discovered the unprotected Elasticsearch cluster, which contained several data collections comprising a total of more than 350 million records including caller names, phone numbers, and locations, among other data. One database included transcriptions of hundreds of thousands of voicemails, many involving sensitive information such as details about medical prescriptions and financial loans.

Broadvoice CEO Jim Murphy gave Comparitech the following statement:

> Broadvoice takes data privacy and security seriously. We learned that on October 1st, a security researcher was able to access a subset of b-hive data. The data had been stored in an inadvertently unsecured storage service Sept. 28th and was secured Oct. 2nd.
>
> The company is taking the following steps to address the situation:
>
> - We launched an investigation and ensured the data had already been secured.
> - We alerted federal law enforcement and offered our full cooperation.
> - We are working with the security researcher to ensure that the data he accessed is destroyed.
>
> At this point, we have no reason to believe that there has been any misuse of the data. We are currently engaging a third-party forensics firm to analyze this data and will provide more information and updates to our customers and partners. We cannot speculate further about this issue at this time.
>
> We sincerely regret any inconvenience this may cause.

Timeline of the exposure

Here's a timeline of events as far as we are aware:

- October 1, 2020: Diachenko discovered the database. This is also the date that the database was first indexed by search engine Shodan.io. The same day, Diachenko sent a responsible disclosure to Broadvoice. He received an automated reply but no further correspondence.
- October 4, 2020: The database had been secured.

At this time, we do not know if unauthorized parties accessed the database during the time it was left available to the public.

What data was exposed?

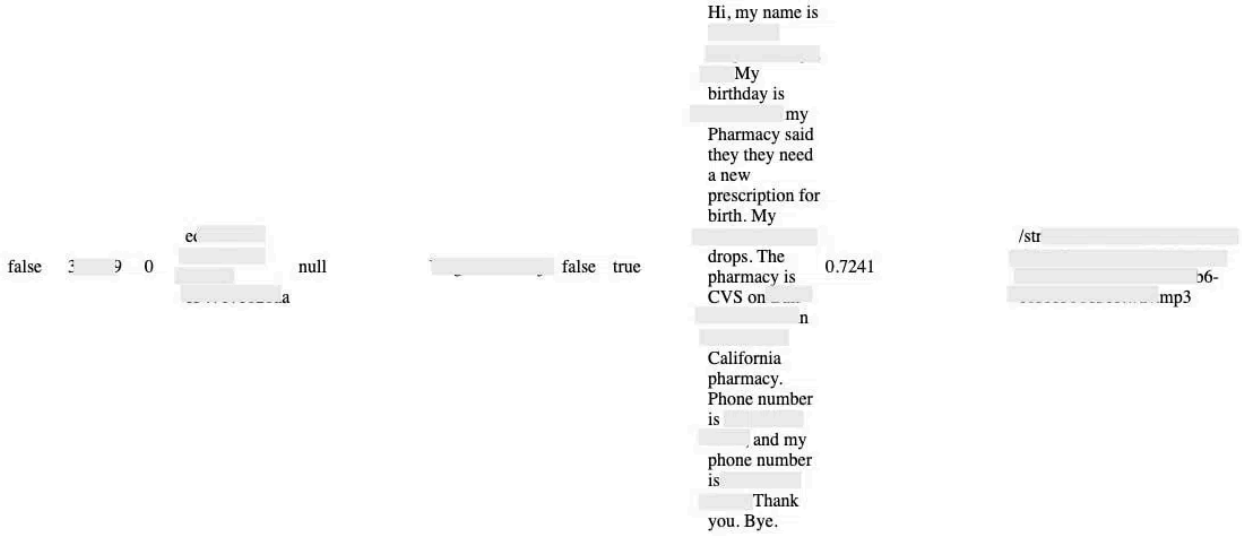
health	status	index	uuid	pri	rep	docs.count	docs.deleted	store.size	pri.store.size
green	open	.tasks	zQiPSQD_TOaFi8S59ymqdw	1	0	36	0	54.9kb	54.9kb
green	open	people	DICY4jJyTpiB4qajfvU6wA	5	0	3454	0	192.4kb	192.4kb
green	open	accounts	gJmwL6ZqQeWPNJFwR_sGrg	5	0	7869	0	2mb	2mb
green	open	quotes	DZu9p4liTE2tYxgF4gTe6w	5	0	32988	0	4mb	4mb
green	open	people-production	YO0agO-LSHm1YbAIanQT5g	5	0	157920	0	66.9mb	66.9mb
green	open	incoming_fax_spoolies	bg0DHRzvSYyB-yWwqttfGQ	5	0	492949	0	93.4mb	93.4mb
green	open	faxes-production	9WACm1cPQCaRpCHljwrCAw	5	0	809847	86725	170.8mb	170.8mb
green	open	voicemails-production	KviAKYBsSDOqwRj_gjbrUQ	5	0	2085308	10260	684.6mb	684.6mb
green	open	cc_cdrs_2	EkcWejLySrillTbnuTolDw	5	0	76979035	0	14.6gb	14.6gb
green	open	ocdrs	pJ0k2wPCTMKwYMO4PV8DDg	5	0	275929319	0	66.6gb	66.6gb

The leaked data was stored in an Elasticsearch cluster that at the time of discovery did not need a password or other authentication to access it. The cluster included around 10 collections, the largest of which held more than 275 million records that included the following:

- Full caller name
- Caller identification number
- Phone number
- State
- City

Another collection held over two million voicemail records, at least 200,000 of which included transcripts. Most of these records contained:

- Caller name (full name, business name, or a generic name such as “wireless caller”)
- Caller phone number
- A name or identifier for the voice mailbox (for example, a first name or general label, such as “clinical staff” or “appointments”)
- Internal identifiers



Many of the transcripts included select personal details such as full name, phone number, and date of birth, as well as some sensitive information. For example, some transcripts of voicemails left at medical clinics included names of prescriptions or details about medical procedures. In one transcript, the caller identified themselves by their full name and discussed a positive Covid-19 diagnosis.

Other voicemails left for financial service companies included details about mortgages and other loans, while there was at least one instance of an insurance policy number being disclosed.


```
{
  "_index": "people-production",
  "_type": "_doc",
  "_id": "7
  "_score": 1.0,
  "_source": {
    "firstName": "
    "lastName": "
    "package": "xbp_legacy",
    "role": "user",
    "email": null,
    "mobileNumber": null,
    "createdAt": "2015-04-24T22:10:15Z",
    "timeZone": "Pacific Time (US & Canada)",
    "vmBoxId": 3
    "accountId": 2
    "locationId": 2
    "agent": false,
    "extension": 8
    "gravatarUrl": "https://www.gravatar.com/avatar/2a
    "primaryLine": {
      "id": 1743,
      "friendlyName": "
      "callerIdName": "",
      "callerIdNumber": "19
      "nickname": "
    },
```


A collection entitled “people-production” appeared to contain account details for Broadvoice users. Looking at account ID numbers, we were able to cross-reference entries with records in other collections. Based on information in this collection, it appears that most, if not all, of the exposed data pertains to users of XBP, a platform that Broadvoice acquired several years ago.

The dangers of exposed data

The leaked database represents a wealth of information that could help facilitate targeted phishing attacks. In the hands of fraudsters, it would offer a ripe opportunity to dupe Broadvoice clients and their customers out of additional information and possibly into handing over money. For example, criminals could pose as Broadvoice or one of its clients to convince customers to provide things like account login credentials or financial information.

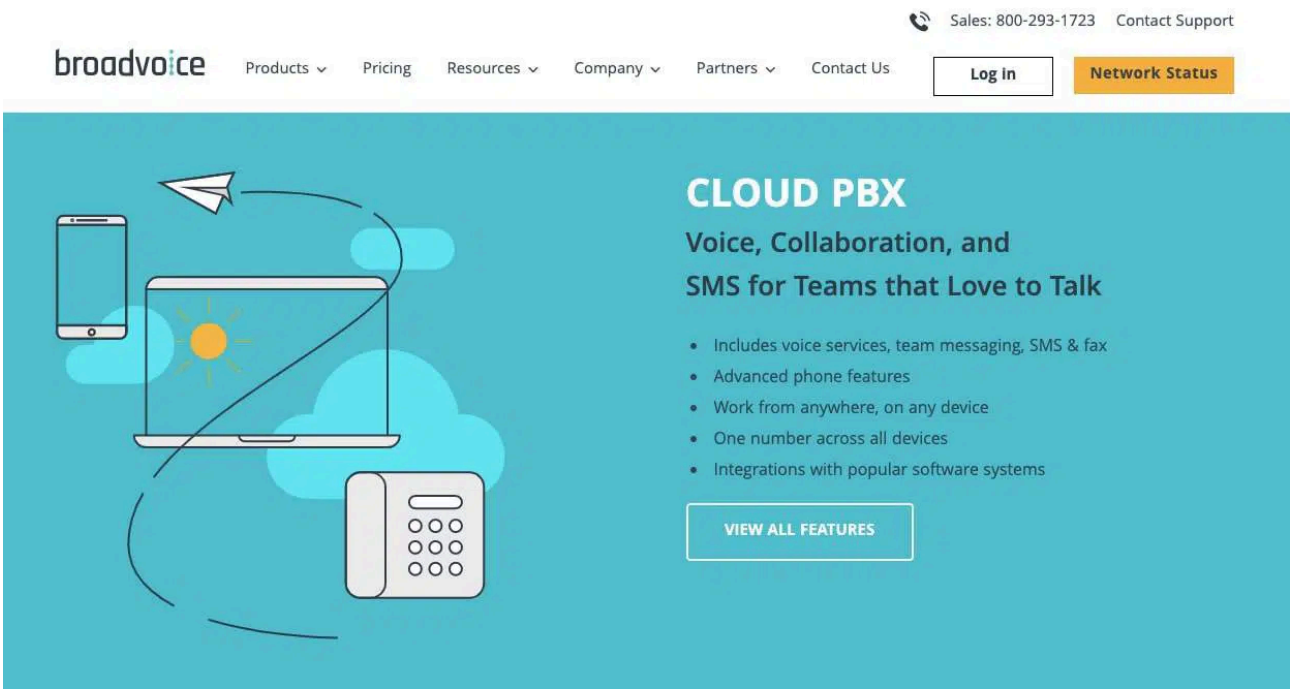
Anyone whose data has been exposed in the leak should be on the lookout for emails, text messages, or phone calls that ask for personal information. You should also avoid clicking on links or attachments in emails or messages unless you absolutely trust the sender.

Of particular concern here are the details in some of the voicemail transcripts. Information about things like medical prescriptions and loan enquiries could be used to make messages extremely convincing and persuasive.

Perhaps more concerning, some details such as insurance policy numbers and enquiries about financial loans could be used in fraud attempts without any need for phishing. Customers should keep a close eye on financial

statements and credit reports.

About Broadvoice



Broadvoice is a communications company offering several services to businesses including cloud PBX (an all-in-one cloud communication platform for connecting with customers), SIP trunking (multimedia IP communication networks), and contact center solutions.

Broadvoice acquired XBP in 2017 to take advantage of its proprietary communications software. It has since retired the XBP brand, but the software remains an integral part of Broadvoice's offerings.

As far as we know, neither company has been involved in a data leak prior to this exposure.

Why we reported this data incident

Security researchers at Comparitech scan the internet looking for accessible databases that hold personal details. When we discover unsecured data, we determine what information is exposed, who it pertains to, who is responsible for it, and what the potential impact of the exposure could be.

We then work quickly to inform responsible parties of the data leak so that the information can be secured. Then, in order to help raise awareness of data exposures in general and inform affected parties of this particular incident, we publish a report (such as this one). Our aim is to have the data secured and all relevant parties informed as quickly as possible to minimize the potential damage caused.

Previous data incident reports

The Comparitech security team has uncovered many breaches similar to this one. Here are some of the reports we've published:

- User logs including passwords of millions of UFO VPN customer exposed online
- Telmate exposes the personal info and messages of millions of prison inmates
- 2.7 billion email addresses and many passwords exposed online
- Exposure involving 600,000 records of Town Sports staff and members
- More than 260 million Facebook credentials leaked on a hacked forum
- Data leak involves over 2.5 million CenturyLink customer records
- Records of almost 8 million UK online purchases leaked
- 42 million phone numbers and user IDs of Iranian Telegram users exposed
- 250 million Microsoft customer records leaked
- Social media broker exposes 235 million scraped profiles

Writer:

Paul Bischoff

Tech Writer, Privacy Advocate and VPN Expert

Paul is Comparitech’s editor and a regular commentator on cyber security and privacy topics in national and international media including New York Times, BBC, Forbes, The Guardian and many others. He's been writing about the tech industry since 2012 for publications like Tech in Asia, Mashable, and various startup blogs. Paul has an in-depth ... Read more

---