Three Vulnerabilities in iBSG 3.5

2023-12-17

#cve

> Table of Contents

> Background

In mid-2023, during the monsoon season, I traveled to Thailand. During my three-week stay, I had the opportunity to admire the stunning natural beauty in the north, the picturesque beaches in the south, and the warmth and culinary expertise of the Thai people. Although this trip was intended as a vacation to clear my mind after several stressful months working as an IT security expert, I discovered three previously unknown security vulnerabilities in the internet gateway software iBSG developed by N.V.K. INTER CO., LTD.. This blog post aims to document these findings, focusing on their discovery, severity, exploitation, and mitigation.

> Objective

From the website of the producer NVK (translated, original in Thai):

> iBSG (Intelligent Broadband Subscriber Gateway) is a complete solution designed specifically for wired and wireless Internet Service Providers. In an apartment, hotel, school or office, iBSG has a main function as Gateway to determine access rights to the Internet, billing system, advanced network management system. Computer traffic data collection system (Traffic Log Recorder) in accordance with the Act. Comp 2007 by iBSG is available in the form of software to be installed on a computer. And a finished hardware (iBSG The Box) at present, iBSG is considered a system that has been highly reliable. And is considered the most popular Internet Gateway solution in Thailand.

From a software perspective, version 3.5 of NVK's iBSG solution is a customized CentOS 6.9 running on Linux kernel 2.6.32. The distributed IBSGLITE_V3.5_32R1B ISO, which is the exact version analyzed in this blogpost, is a customized and kickstarted CentOS installation ISO which automatically installs the system and iBSG software to the first available hard drive without the need for user interaction.

Given that the software is designed for use with iBSG hardware or at least a headless computer, this automated kickstart method is logical, as it allows for updates or reinstallation without needing to connect a keyboard, mouse, or display to the device. However, this approach limits the system owner's control over underlying configurations, such as the root password, disk encryption, or SSH settings.

> Timeline

- XX-07-2023: Discovery of vulnerabilities on own VM in lab environment
- 03-08-2023: Initial disclosure towards NVK
- 08-08-2023: Disclosure of technical details towards NVK
- 21-08-2023: CVEs assigned

- 17-12-2023: Release of blog post

> Lab Setup

As the iBSG software is not resource hungry, it can be easily installed into a small VM (I found 1C with 1GB memory and 5GB HDD sufficient) simply by booting off the ISO and letting the installer do the rest.

Attach a Host-only network to the machine and configure your host machine appropiately, e.g. with 192.168.2.23/24. After installation, iBSG configured the first network interface with IP 192.168.2.254/24.

Note that the kickstarted ISO is set up to automatically encrypt the HDD and set a password for the root user:

```
# From IBSGLITE_V3.5_32r1B_[B0850894]_U_C69.ISO/default.cfg, L5,12
rootpw --iscrypted $1$4Tmm01jl$7HRvcW.bz7uGmX9hiQWvR.
[...]
bootloader --location=mbr --append="crashkernel=auto pcie_aspm=off" --md5pass=$1$eE
```

This configuration prevents logging into the VM via the console. To gain further access to the system, I modified these lines to enable access:

```
  # do not crypt / :
  sed -i 's/bootloader --location=mbr --append="crashkernel=auto pcie_aspm=off" --

  # set root password to "oinkoink"
  sed -i "s/rootpw --iscrypted \$1\$4Tmm01jl\$7HRvcW.bz7uGmX9hiQWvR./rootpw oinkoi
```

Side note: using sed in such a scenario should be avoided. As you can see, you need to match the length, and this method would fail if there were a checksum algorithm in place. The clean solution would've been to use mkisofs and create a new ISO, but hey, I was on vacation and sed worked in this case.

After installation, you can further inspect the disk by running:

- `sudo losetup --find --partscan ./hdd_after_install.img`
- `sudo vgchange -ay vg_ibsg`
- `sudo mount -o defaults,ro /dev/vg_ibsg/lv_root /mnt`

Nearly all of the iBSG-specific software is in `/home/ibsg`:

- `bin`: scripts mostly called by cron or doing helper stuff
- `class`: PHP class files to be imported by the web frontend
- `conf`: miscellaneous content and auxiliary files (not only configs!)
- `install`: scripts used in the first run, driver stuff
- `webui`: directly hosted via HTTP on port 80/TCP

All PHP files are obfuscated using ionCube. While there are dubious online services offering to decrypt the source code, I strongly advise against using them due to legal and security concerns. Please note that I am not a lawyer. For this blog post, we will treat the source code as a black box.

> Vulnerabilities

>> CVE-2023-39807

>>> Description

Unauthenticated blind SQL injection (SQLi) in `/portal/user-register.php` allows remote attackers to read out administrator usernames and unhashed passwords through the `a_passwd` POST parameter.

>>> Evaluation

CVSS v2: AV:N/AC:L/Au:N/C:C/I:C/A:C = Base Score **10.0**

From my perspective, a vulnerability able to retrieve administrator credentials on this service is the most critical problem you can have, also taking into consideration that the passwords are not hashed. This also allows lateral

movement in the network, especially when chained with the command injection vulnerability described below.

>>> Exploitation

The process of exploiting the blind SQL injection using SQL's `sleep` command can be automated with the excellent sqlmap tool:

```
sqlmap --method=POST --data="a_passwd=%INJECT HERE" --url http://192.168.2.254/p
```

This command will extract the `a_login` and `a_passwd` columns from the `admin` table in the `ibsg` database.

>>> Mitigation

If available, filter user input using a web application firewall.

Ensure that admin usernames and passwords are not reused across other services and systems. Update your current credentials.

Install the update provided by NVK.

>> CVE-2023-39809

>>> Description

Authenticated blind command injection (OSi) in `/manage/network-basic.php` allows remote attackers to execute commands as root user, escalating from the iBSG administrator account on the web portal to the OS administrator, through the `system_hostname` parameter.

The affected endpoint is accessed within the admin web portal under `/manage` when navigating to `Network/Basic/Miscellaneous`. While the `Hostname` field value, equivalent to the `system_hostname` parameter, is filtered client-side,

preventing attacks through the UI, the endpoint itself does not filter the input, allowing blind remote code execution.

>>> Evaluation

CVSS v2: AV:N/AC:L/Au:N/C:C/I:C/A:C = Base Score **8.5**

>>> Exploitation

To change the root password, execute the following command:

```
curl 'http://192.168.2.254/manage/network-basic.php' -X POST -H 'Referer: http:/
```

Be sure to replace the session cookie with your own. It may also be helpful to adjust other settings to match your current environment; the values provided are specific to my lab setup and may vary in yours.

The command above sets the hostname to `ibsg.nvk$(usermod -p Y7.uTy24W3PjI root)`, which changes the root password to `md5crypt Y7.uTy24W3PjI`, corresponding to `oinkoink` in plaintext. Interestingly, while the entire hostname is altered to this string (without executing the enclosed `usermod` command), the command still runs, likely in a separate code block.

After running the above command, you can use SSH to log into a proper shell.

>>> Mitigation

To ensure your current installation is not compromised, perform a clean reinstall.

Install the update provided by NVK.

>> CVE-2023-39808

>>> Description

Fixed unchangeable root password and SSH misconfiguration allow attackers to take over all installations of iBSG 3.5.

During installation, the password hash `$1$4Tmm01jl$7HRvcW.bz7uGmX9hiQWvR.` (md5crypt) is set as the root password hash. This password is neither randomized per installation nor can it be changed through the web interface on `/manage` (though it can be altered using the OSi mentioned in CVE-2023-39809).

The system uses OpenSSH version 5.3p1, which is over a decade old. The main issue lies in the absence of a `PermitRootLogin` directive in the `sshd_config` file, leading to the default setting being applied. Modern SSH versions default to `prohibit-password`, but this older version defaults to `yes`, permitting anyone with the correct root password to log in.

>>> Evaluation

The password hash is publicly known and the same on all installations of iBSG v3.5. This is basically a backdoor for anyone with enough hash cracking capacity or with the right password. While NVK as a company won't have a proper attack scenario to be a realistic threat in this case, the password could be leaked or stolen and would pose an immediate and high risk to any iBSG installation.

Using 4 RTX3090s in parallel would still take 1.9846145346006685e+24 years in the worst case to crack this hash, so take the risk of hash cracking with a grain of salt. If the cleartext password is not a randomized string but e.g. a word or sentence in Thai, it could still be a matter of minutes to crack it though.

>>> Exploitation

Unless you possess a NVIDIA Tesla cluster: not applicable.

>>> Mitigation

To ensure your current installation is not compromised, perform a clean reinstall.

Install the update provided by NVK.

>> Other Observations

SNMP (161/UDP) is open, which is handy, but also exposes a lot of information about the system. Evaluate if you really need SNMP to be opened, and close it via firewall rules otherwise. My attempts to use the SNMP RCE trick were unsuccessful, which doesn't mean that it doesn't work - again, I was on vacation… :)

>> Chaining and Overall Evaluation

Combining CVE-2023-39807 and CVE-2023-39809 enables an attacker to escalate from an unauthenticated remote position to an authenticated administrator with full shell access. While this is the most apparent chain, utilizing either CVE alone for lateral movement within the network is also feasible. Password reuse remains a significant issue, exacerbated by the cleartext nature of passwords in iBSG.

> Conclusion

It was a lot of fun to dig my way through this black box. I am used to having something in my hands to reverse engineer, which was not possible in this case, so I learned a lot on the way.

Thank you for reading!

Now, install the fix provided by NVK for iBSG 3.5, and consider visiting Thailand! :)