SSD Advisory – iBall Multiple Vulnerabilities

blogs.securiteam.com/index.php/archives/3654

Vulnerabilities summary
The following advisory describes two (2) vulnerabilities found in iB-WRA150N devices, firmware 1.2.6 build 110401 Rel.47776n.

iB-WRA150N is "a powerful solution to Internet connectivity at home, small offices and work stations. The key is if you are using an ADSL2+ connection now and later decide to change to Broadband or vice-versa you don't need to change your router. This iBall router is 2-in-1 and compatible to both – Broadband connection as well as ADSL2 connection (Telephone connection or cable operator connection). "

The vulnerabilities found are:

- Hard coded accounts
- Remote command execution

Credit
An independent security researcher, maxki4x, has reported this vulnerabilities to Beyond Security's SecuriTeam Secure Disclosure program.

Vendor response
We tried to contact iBall since December 20 2017, repeated attempts to establish contact were answered, but no details have been provided on a solution or a workaround.

Vulnerabilities details

Hard coded accounts
Username: admin
Password: admin

Username: support
Password: support

Username: user
Password: user

Remote command execution
After we logged in to the victims router – using the hard coded accounts, we can trigger the second vulnerability and achieve remote command execution.

User controlled input is not sufficiently filtered, allowing user to inject arbitrary commands into ping test arguments in Diagnostics page.

By entering the following input in the ping test arguments in Diagnostics page, the attacker can get the /etc/passwd file:

```
1  127.0.0.1;cat/etc/passwd
```