Security News
2011-41018 GoAhead Webserver Stored XSS Vulnerability

1. Affected Version

GoAhead Webserver

2. Description

1. The GoAhead WebServer is a standards-based Web server designed for cross-platform support. While WebServer is designed for embedded devices it is nevertheless a fully functional web server and its use is not limited to embedded devices.

2. There are several stored cross-site scripting vulnerabilities found in GoAhead WebServer can be exploited to execute arbitrary JavaScript.

3. Vulnerability Analysis

The proof-of-concept code is listed as follows:

```
POST /goform/AddGroup HTTP/1.1
group=<script>alert</script>&privilege=4&method=1&enabled=on&ok=OK
```

Table 1: The proof-of-concept code

This flaw is caused due to improper validation of POST requests by the addgroup.asp, addlimit.asp and adduser.asp scripts. A remote attacker with access to the GoAhead Webserver can conduct a cross site scripting attack, which could be used to result in information leakage, privilege escalation, and/or denial of service.

4. Recommendation

1. Lionic IDP signature database can prevent this attack since 12/10/2011.
2. Upgrade to the latest non-affected version of the software.

5. Reference

1. http://www.kb.cert.org/vuls/id/384427