Security Advisory

Inteno ICE-CLIENT

12th of February 2015

Juan J. Güelfo
CEO & Lead IT-security consultant 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

- ***12th of February 2015***
  Public disclosure.

- ***12th of January 2015***
  Vendor acknowledges the vulnerability and informs Encripto that the software package has been updated.

- ***10th of January 2015***
  Vulnerability discovered by the researcher and details shared with the vendor.

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, ICE-CLIENT (iopsys Communication Engine) is an XMPP communication engine with application modules that enable services like WiFi Joe, File Me, Home Watch & Home Control. It also has a pairing function to iopsys portal.

Iopsys is an open source based software platform for embedded devices developed by Inteno. Iopsys key components include CPE software, packet engine, SDK and a cloud based application portal.

2. Summary

ICE-CLIENT version 3.0.0-RC5 is vulnerable to web directory traversal. The vulnerability could be exploited by unauthenticated attackers. Successful exploitation would allow attackers to retrieve arbitrary files from the gateway's memory, including "/etc/passwd" and "/etc/shadow".

3. Affected Products

ICE-CLIENT version 3.0.0-RC5, originally found in an Inteno DG150B router.
Other products or previous versions may also be vulnerable.

4. Vulnerability and Proof of Concept (PoC)

The ICE-CLIENT service is started at boot time, and it exposes a web server on port TCP 40124 by default. This web server is vulnerable to directory traversal, allowing access to internal files, including configuration files, "/etc/passwd" or "/etc/shadow".

As a Proof of Concept (PoC), please visit the following URL with a browser:
http://192.168.1.1:40124/etc/passwd

This PoC is assuming that the vulnerable router is located at 192.168.1.1.

The contents of the "/etc/passwd" file should be displayed on the screen. Such file should include the root password in encrypted (DES) form. From here, the root credentials could be cracked in a reasonable amount of time. Other files could be retrieved with the same technique as well.

5. Remediation

The vendor has released a new firmware version that addresses the issue.
Users are encouraged to update their devices with the latest firmware available in order to patch the vulnerability.

6. Credit

The vulnerability was originally discovered in an Inteno DG150B 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/