

# [Full-disclosure] Web-style Wireless IDS attacks

---

*Source:* <http://www.derkeiler.com/Mailing-Lists/Full-Disclosure/2006-10/msg00419.html>

---

- *From:* [noreply@xxxxxxxxxxxxxx](mailto:noreply@xxxxxxxxxxxxxx)
  - *Date:* Fri, 20 Oct 2006 16:14:20 +0400
- 

Web-style Wireless IDS attacks

By Sergey Gordeichik, Positive Technologies Security Expert

## Introduction

Wireless intrusion detection systems (WIDS) are not yet as popular as their wired counterparts, but current trends would suggest that their number is set to grow. One positive factor in this respect is the integration of such programs with active network equipment and Management awareness of the risks associated with the unauthorised use of wireless devices. This awareness has led to an increase in the number of WIDS installations – even where wireless networks are not used.

In view of this situation, specialists in the field of security are now aware of the need to evaluate not only the quality features of any product, but also of the need to predict any possible negative influence arising from its implementation on the security of a corporate network.

This article looks at the results of research into wireless intrusion detection systems from the point of view of the specialist in the field of applications security. Design faults discovered are not discussed in the article as their correction requires significant effort on the part of the manufacturer.

Full article:

<http://maxpatrol.com/webwids.asp>

---

Full-Disclosure – We believe in it.

Charter: <http://lists.grok.org.uk/full-disclosure-charter.html>

Hosted and sponsored by Secunia – <http://secunia.com/>