



Australian Government

Attorney-General's Department



AUSTRALIA'S NATIONAL
COMPUTER EMERGENCY RESPONSE TEAM

CERT Australia Industry News

Wind River VxWorks Vulnerabilities.

Two security vulnerabilities have been publically announced in the real-time operating system VxWorks [1]. This operating system is widely used in embedded devices such as networking equipment. Businesses may need to check whether they systems are vulnerable and take steps to patch or mitigate.

Technical Details

The first vulnerability [2] is due to a listening debug service on UDP port 17185. This service can be used by remote unauthorised attackers to execute commands and take complete control of the device.

The second vulnerability [3] is due to a weak hashing algorithm used in the standard authentication API. The weakness can cause different password strings being represented as the same hash, which is known as a collision. As a result it could be easier for attackers to successfully conduct brute force attacks.

Business Impact

Devices that are running VxWorks with the affected debugging service open are vulnerable to numerous attacks ranging from remote code execution to denial of service. It may also be possible for attackers who take control of these devices to monitor network traffic which may expose sensitive information such as user credentials. The vulnerability is trivial to exploit and will also have exploit code released in the near future. The second vulnerability would make it easier for attackers to break into remote services such as FTP.

Businesses should contact their vendors to determine if their systems are affected and check that they are running the most current firmware version for their devices. The first vulnerability can be mitigated easily by blocking access to this port through your firewall. The second vulnerability can be mitigated by white listing access to your remote services or disabling them if they are not in use.

Further Reading

[1] <http://www.windriver.com/products/vxworks/>

[2] <http://www.kb.cert.org/vuls/id/362332>

This document remains the property of the Australian Government. The information contained in this document is for the use of the intended recipient only and may contain confidential or privileged information. If this document has been received in error, that error does not constitute a waiver of any confidentiality, privilege or copyright in respect of this document or the information it contains. This document and the information contained herein cannot be disclosed, disseminated or reproduced in any manner whatsoever without prior written permission from the Assistant Secretary, E-Security Policy and Coordination, Attorney-General's Department, 3 - 5 National Circuit, Barton ACT 2600.

The material and information in this document is general information only and is not intended to be advice. The material and information is not adapted to any particular person's circumstances and therefore cannot be relied upon to be of assistance in any particular case. You should base any action you take exclusively on your own methodologies, assessments and judgement, after seeking specific advice from such relevant experts and advisers as you consider necessary or desirable. **To the extent permitted by law, the Australian Government has no liability to you in respect of damage that you might suffer that is directly or indirectly related to this document, no matter how arising (including as a result of negligence).**