Applied Risk

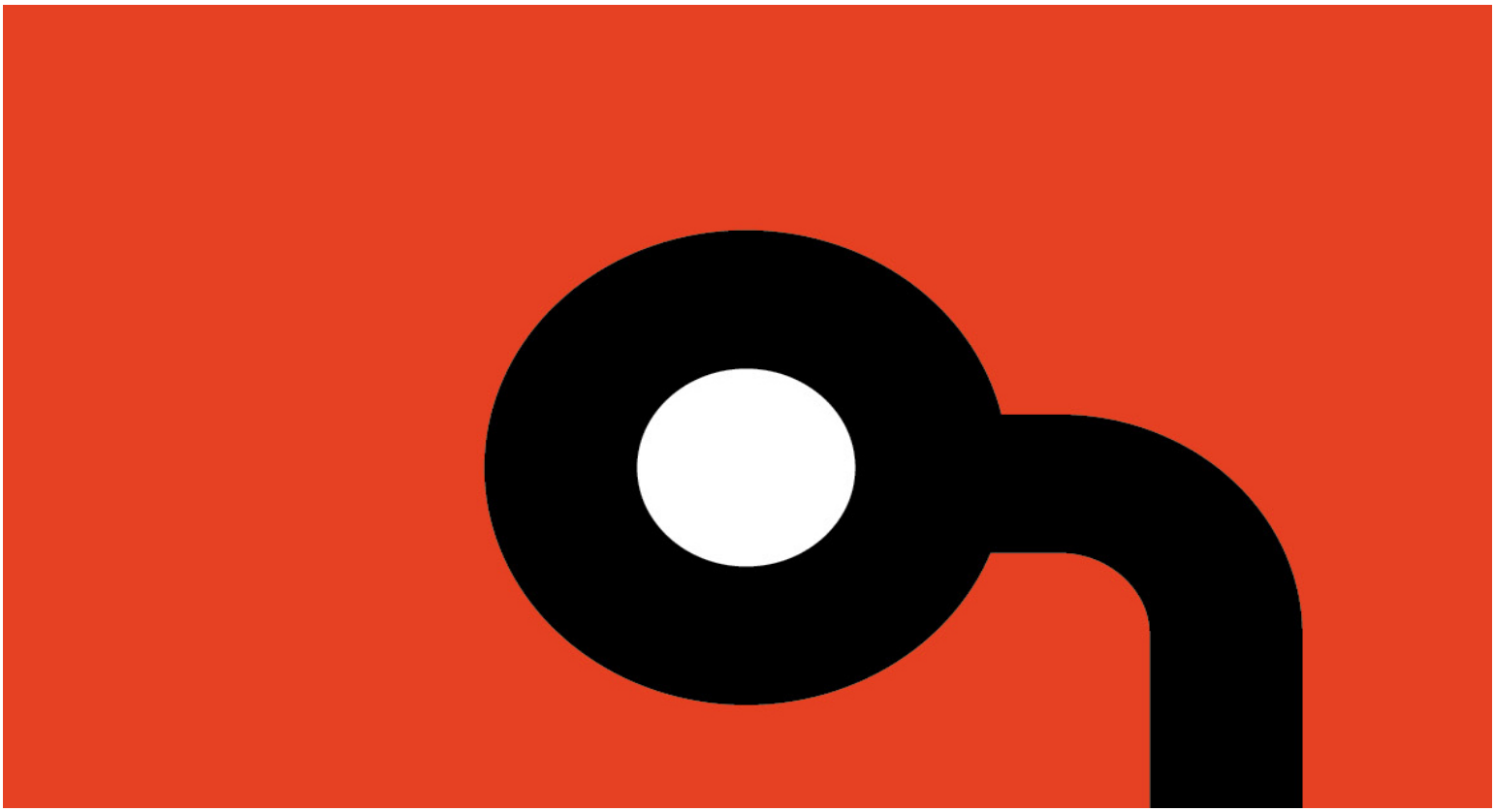
ARA-2014001

Authorization Bypass in mGuard Series Industrial Security Router

Severity: High

Release Date: June 30, 2014

Classification: Unrestricted



OVERVIEW

Researchers of Applied Risk discovered authorization bypass vulnerability in the mGuard series Industrial Security Router products that can lead to sensitive information disclosure such as system configuration settings and credentials (CVE-2014-2356, ICS-VU-311092).

The mGuard is an industrial security solution designed for protection of Industrial Ethernet Networks and secure remote maintenance of ICS/SCADA systems via internet.

AFFECTED PRODUCTS

The following product lines and firmware versions are affected:

- Innominate mGuard rs2000/rs4000/delta/centerport
- Phoenix Contact FL MGUARD rs2000/rs4000
- Hirschmann EAGLE mGuard

Innominate has confirmed firmware versions starting from 4.0 and up to 8.0.2 are vulnerable. This vendor has fixed this issue in respectively firmware and update packages version 8.0.3, 8.1.0 and 7.6.4.

This vulnerability has been discovered and validated on Phoenix Contact rs4000 with firmware version 7.5.0. Since the several brands and models share the same firmware codebase it is highly likely that the discovered vulnerability is present across the entire mGuard product line, but at the time of publication no official confirmation was received from Belden and Phoenix Contact.

IMPACT

An attacker could obtain full diagnostics information consisting of configuration and log files. These files contain the following potentially sensitive information:

- SNMP community strings;
- Users Credentials;
- Firewall ruleset;
- Internal hostnames and IP addresses.

The vulnerability is remotely exploitable and could allow an attacker to map internal networks and identify potential targets as part of reconnaissance activities.

BACKGROUND

Innominate is a German-based company that sells products worldwide through its international partners. Innominate was acquired by Phoenix Contact in 2008.

VULNERABILITY DETAILS

For diagnostics purposes the mGuard allows a logged in user to create a ‘diagnostics configuration snapshot’. By sending a crafted URL an attacker can circumvent the authorization checks and create and download such a snapshot without the need of a valid logon session.

MITIGATION

If possible, Innominate customers should either upgrade to the latest firmware or install the latest update package. Innominate has released its own advisory titled “Security Advisory 2014/06/26” discussing this vulnerability which can be found on the vendor website.

Currently there is no known vendor patch available for Hirschmann and Phoenix Contact branded mGuard devices. However, the risk of this vulnerability being exploited by external attackers can be mitigated by restricting network access to the device’s web interface. It is highly recommended to never expose the device’s web management interface directly to the Internet. Instead use the built-in VPN feature to connect to the internal interface address.

REFERENCES

Innominate Security Advisories
http://www.innominate.com/data/downloads/software/innominate_security_advisory_20140626_001_en.pdf

Innominate
http://www.innominate.com/en/products

Phoenix Contact
https://www.phoenixcontact.com/online/portal/us?1dmy&urile=wcm:path:/usen/web/main/products/subcategory_pages/Security_routers_and_firewalls_P-08-08-09/

Hirschmann
http://www.e-catalog.beldensolutions.com/link/57078-24455-49853-24491/en/conf/0?items=30

CONTACT DETAILS

For any questions related to this report, please contact Applied Risk Research team at:

Email: research@applied-risk.com

PGP Public Key:

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
mQENBFOgiBQBCACj+Notofe/liuHuc90yy8GAfFn8YFCsMCo7wQmQRNTT43bZQq2
gQr7FTLtOl6rBkOLm8bDk0YY/CtWsjdLh1jlDrWyfU6yIzfcu4CSpn1+5n1ivNN5
17ri+VtmgF392twiKhy2+MC9O4of+GMyu1hy5pIjwi3qGzdNlAnT7m7U/hNzaIR4
ae7+NuWtEvWWKyp3IEEMKTDV/ZOtRD1tfIR8KeBB7Axa8cJdlotw/Ail9TLVB6kt
a/BlvhM/zgWfbEPadnx6B0u7pdW50bTECAs0VHje8mcheTwTCAJo+de3/DqUA34X
oF9aAZWpZWE7VH0O4Q8ZtfrXPFqR2xF8LHhZABEBAAG0REFwcGxpZWQgUmlzayBS
ZXNlYXJjaCBUZWFtIChubyBwYXNzd29yZCkgPHJlc2VhcmNoQGFwcGxpZWQtcmlz
ay5jb20+iQE+BBMBAgAoBQJToIgUAhsjBQkJZgGABgsJCAcDAgYVCAIJCgsEFgID
AQIeAQIXgAAKCRA6nyA79MpeSay8CACSI4UhAget5Z+qEDmz1fe+9krgmx7wwDnF
ig4AVICU8ppJQoUCB5pP6eIV/DM7i+mu8e9zeGlA82t69yTVIANWx72zPmGn5Ku8
4t79gR8V+99PW+O+1rej+96wfL2v+IuOXOcJkTsheUyQZ8Klwc1U8kTdGZEY+/IZ
c32ZhyJ04/cchVP/Zsj2WQIh84wbqa27bTEyyFBnD8FdQ2R4UDTqwACbLgp82m29
P346s80c15RZIX8wUAu0LcNbWJJHRsX6Sa+MozTNug9yWdpZt+nmHEMl95lJYktR
w3+gwyaXeUxALX8Baq2EJDdNx9OlsryiNFdnE9vKIM0+24fTDoqguQENBFOgiBQB
CACtSAm5oBD4kJJY+rtHh6xoytOzP6bFEnrVjqXrXCj+ECG6+N6Droqd072X5hki
qoL1viI4NV+2jrYTtMIu+/nc4zuUFUDRYSm0X/K3WgsqaLA4jdedTm45Tau/Fn6W
26tB5AaddcoDdx6JVGIxFvwU+41KoZ7ouDZo7UEBZ7getPubyR4aPepUsjYnPOUL
0SHH76+b/pC5AZm4crpqWf7Q+qaYQdBIhJbgm5ijFzCyHusYgVGBT1hak81QGpM0
1K9wXki/fJrRyEsWWUjpVSEPRizsFJ60v+NrX50gvvXed8MlX0O9efwgeCmGIVDL
oxF/AmnznYWy0LYWAhh/dW7dABEBAAGJASUEGAECAA8FAlOgiBQCGwwFCQlmAYAA
CgkQOp8gO/TKXkmgdQf/ZtwhL2bs+mlmTUmlT3XO4ekVPRLQKtBYfr8y4rdfnq7Y
MdFYEJAt45R+e4I3I7cIJM1/ImncjFng1EpwFItAXVLa1ktiO6BqT6wBqL6pSBe3
2x5VP8OEnnRubCgYaTotNfiEErgh8cG92tW/TiQArU2dnBcVwYHVwPm450pEv9Aq
BBzgeZ25I1Cv0vlQkQLy9PuTA6DWoxeIxbaMD8ZpKGi+XDrfguJ3tERQMlUA6Fc+
OBkT/NKz8mgecVrwCWbCmScyEhh6onTkevI+mydvsxYG8rE6YVxl3oK5Xi6tvAt9
cUPKKK363nkA1AEoMvTz1bCbmTGvTNWLifoMNtNnGA==
=pAvd
-----END PGP PUBLIC KEY BLOCK-----
```