AR2019006

Nortek Linear eMerge 50P/5000P 4.6.07 Multiple Vulnerabilities

Author: Gjoko Krstic

Release Date: May 10, 2019

Copyright Notices

COPYRIGHT NOTICE

OVERVIEW

Multiple vulnerabilities were found in the Nortek Linear eMerge 50P/5000P Access Control Platform. These findings include Default Credentials, Directory Traversal, Cross-Site Request Forgery, Authentication Bypass, Unauthenticated File Upload and Command Injection.

AFFECTED PRODUCTS

Linear eMerge 50P/5000P;

The following versions are affected:

- 4.6.07 (revision 79330) and below

The vulnerabilities have been discovered and validated in Linear eMerge 50P/5000P 4.6.07. Older versions are affected too.

IMPACT

An unauthenticated user can have full system access.

BACKGROUND

Nortek Security & Control, LLC (NSC) is a leader in wireless security, home automation and personal safety systems and devices. The Linear eMerge 50P/5000P blends advanced capabilities with ease of configuration and use for small to mid-sized commercial and high-end residential applications. eMerge integrates credential-based access control, intrusion detection, and video surveillance for a small to mid-sized facilities.

VULNERABILITY DETAILS

Default Credentials

Attackers can easily obtain default passwords and identify Internet-connected target systems. Passwords can be found in product documentation and compiled lists available on the Internet. It is possible to identify exposed systems using search engines like Shodan, and it is feasible to scan the entire IPv4 internet.

Applied Risk has calculated a CVSSv3 score of 9.8 for this vulnerability. The CVSS vector string is CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H.

Directory Traversal

The application suffers from a Directory Traversal vulnerability. The software uses external input to construct a pathname that should be within a restricted directory, but it does not properly neutralize sequences such as “../” that can resolve to a location that is outside of that directory. This allows attackers to traverse the file system to access files or directories that are outside of the restricted directory.

Applied Risk has calculated a CVSSv3 score of 9.8 for this vulnerability. The CVSS vector string is CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H.

Command Injection

The application constructs an OS command using externally-influenced input from an upstream component, but incorrectly neutralizes special elements that could modify the intended OS command when it is sent to a downstream component. This could allow attackers to execute unexpected, dangerous commands directly on the operating system.

Applied Risk has calculated a CVSSv3 score of 10.0 for this vulnerability. The CVSS vector string is CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H.

Unrestricted File Upload

The vulnerability exists due to the absence of file extension validation when uploading files through the firmware upgrade upload script. A remote and unauthenticated attacker can upload files with arbitrary extensions into a directory within the application's web root and execute them with privileges of the web server.

Applied Risk has calculated a CVSSv3 score of 10.0 for this vulnerability. The CVSS vector string is CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H.

Cross-Site Request Forgery

The affected application allows users to perform certain actions via HTTP requests without performing any validity checks to verify the requests. This can be exploited to perform certain actions with administrative privileges if a logged-in user visits a malicious web site.

Applied Risk has calculated a CVSSv3 score of 5.0 for this vulnerability. The CVSS vector string is CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:L.

Authentication Bypass

The vulnerability exists due to insufficient validation of input data in authentication mechanism. A remote attacker can send a specially crafted HTTP request abusing the Cookie header value traversing to an arbitrary session file that bypass authentication checks and gain unauthorized access to the application.

Applied Risk has calculated a CVSSv3 score of 8.1 for this vulnerability. The CVSS vector string is CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H.

MITIGATION

Nortek is aware of the reported vulnerabilities but hasn't produced a patch.

REFERENCES

Vendor website

https://www.nortekcontrol.com/

Product page

https://www.nortekcontrol.com/products/access-control-systems/emerge-browser-managed-access-systems-2/

Common Vulnerability Exposure (CVE):

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-7266
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-7267
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-7268
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-7269
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-7270
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-7271

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-----
```