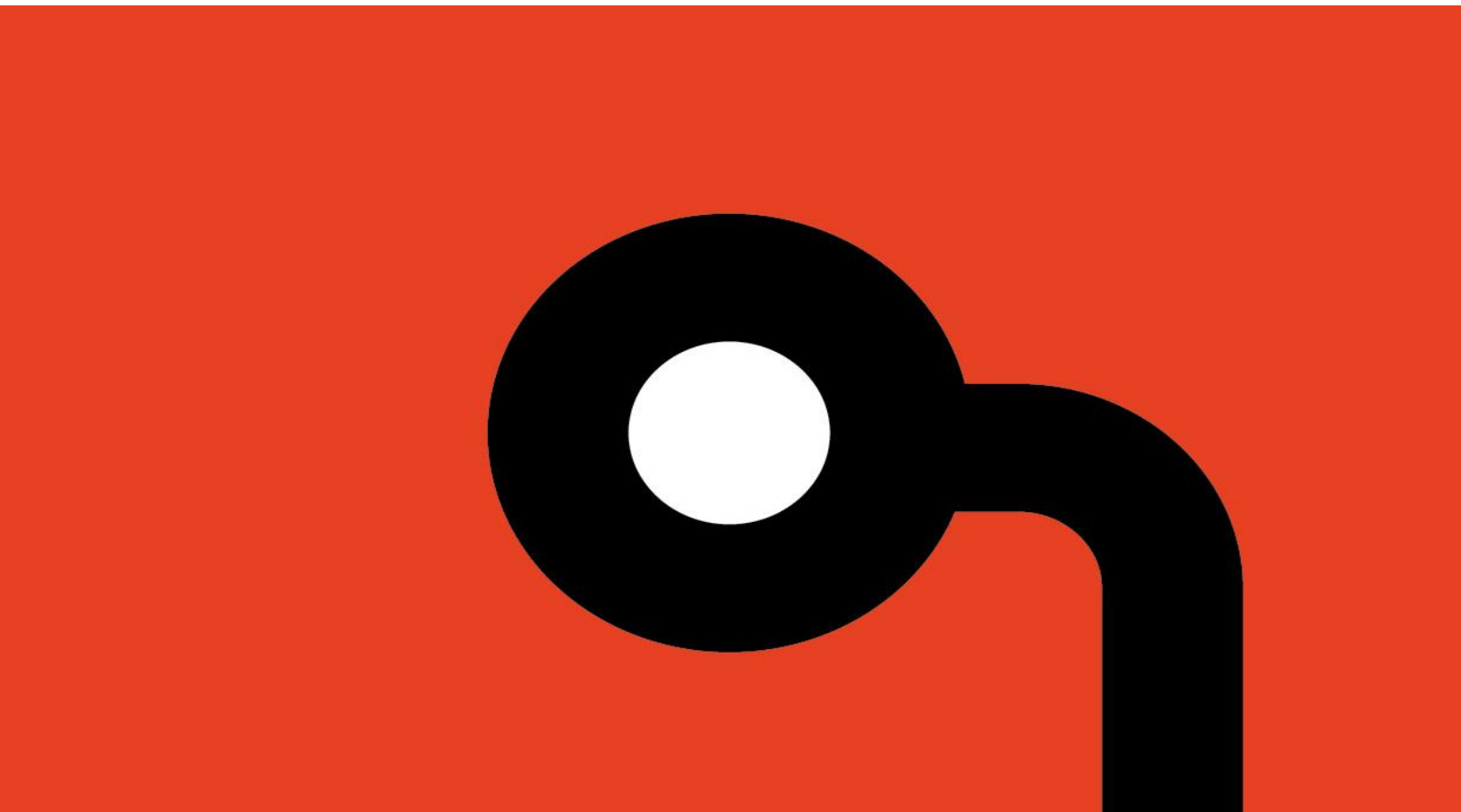
Applied Risk

AR2019005

Nortek Linear eMerge E3-Series 1.00-06 Multiple Vulnerabilities

Author: Gjoko Krstic

Release Date: May 10, 2019



Copyright Notices

OVERVIEW

Multiple vulnerabilities were found in the Nortek Linear eMerge E3-Series Access Control Platform. These findings include Default Credentials, Directory Traversal, File Inclusion, Cross-Site Scripting, Command Injection, Unrestricted File Upload, Privilege Escalation, Authorization Bypass, Insecure Storage of Sensitive Information, Hard-coded Credentials, Cross-Site Request Forgery, Version Control Failure, Stack-based Buffer Overflow and Root Access over SSH.

AFFECTED PRODUCTS

Linear eMerge E3-Series;

The following versions are affected:

- 1.00-06 and bellow

The vulnerabilities have been discovered and validated in Linear eMerge E3-Series 1.00-06. Older versions are affected too.

IMPACT

An unauthenticated user can gain full system access.

BACKGROUND

Nortek Security & Control, LLC (NSC) is a leader in wireless security, home automation and personal safety systems and devices. The eMerge E3-Series represents the next step in the evolution of Linear's access control platform, delivering faster set-up, enhanced features, and industry-leading scalability that outperforms the competition. The E3-Series embedded browser-based network appliance platform makes advanced security technology reliable and affordable for any entry-level access control application.

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.

Cross-Site Scripting

The application suffers from a reflected XSS vulnerability. The issue occurs when input passed via several parameters to several scripts is not sanitized before returned to the user. This can be exploited to execute arbitrary HTML and script code in a user's browser session in the context of an affected site.

Applied Risk has calculated a CVSSv3 score of 5.4 for this vulnerability. The CVSS vector string is CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N.

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 badge image upload script. A remote and unauthenticated attacker can upload files with arbitrary extension into directory within 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.

Privilege Escalation and Authorization Bypass

The application suffers from a privilege escalation vulnerability from view-only to super user privileges. This allows a low-privileged attacker to escalate privileges to the Super User role by changing the POST parameter 'UserRole' value to 1.

The authorization bypass occurs when an authenticated attacker visits a specific GET request against the target that results in disclosing administrative credentials in clear-text. This allows the attacker to re-login with admin privileges and have full access to the control interface.

Applied Risk has calculated a CVSSv3 score of 8.8 for this vulnerability. The CVSS vector string is CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H.

Clear-text Storage of Passwords and Hard-coded Credentials

The application stores passwords in clear-text in its DBMS system. Storing a password in plaintext may result in a system compromise. Hard-coded credentials are also present in plenty of binaries that are

bundled in the firmware OS. These hard-coded credentials typically create a significant hole that allows an attacker to bypass the authentication that has been configured by the software administrator.

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.

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.

Version Control Failure

The solution is failing regarding the version control of the firmware updates. Several updates have changes in the code, but from the other hand, some of the updates are still with old code and without version number changed. This represents a failure in version control approach for the affected product.

Stack-based Buffer Overflow

A stack-based buffer overflow exists affecting several CGI binaries. The vulnerability is caused due to a boundary error in the processing of a user input which can be exploited to cause a buffer overflow. Successful exploitation could allow execution of arbitrary code on the affected device.

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.

Root Access over SSH

The access control platform has SSH enabled with hard-coded credentials for the root account. This allows an unauthenticated attacker to initiate a secure connection with highest privileges (root) and gain full system access.

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.

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/e3emerge/index.php

Common Vulnerability Exposure (CVE):

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-7252
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-7253
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-7254
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-7255
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-7256
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-7257
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-7258
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-7259
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-7260
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-7261
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-7262
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-7263
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-7264
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-7265

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-----
```