

Nice Linear eMerge Command Injection Vulnerability

Industrial access control system- Patch now

<https://www.cisa.gov/news-events/ics-advisories/icsa-24-065-01>
 CVEs: CVE-2019-7256

The vulnerability tracked as CVE-2019-7256 affecting an access control system called Linear eMerge E3-Series is affected by an OS command injection flaw that could allow an attacker to cause remote code execution and full access to the system.

Background The Nice Linear eMerge E3-Series is a popular access control system used in various commercial and industrial environments worldwide which emphasize the importance of the potential widespread impact of this vulnerability specially when the exploit has been publicly available. CVE-2019-7256 received a severity score of 10/10, and can be exploited remotely with low complexity.

Announced March 05, 2024: CISA released an ICS advisory relating to multiple vulnerabilities affecting Nice Linear eMerge E3-Series including CVE-2019-7256 which is exploited in the wild.
<https://www.cisa.gov/news-events/ics-advisories/icsa-24-065-01>

March 25, 2024: CISA added CVE-2019-7256 to its known exploited catalog
<https://www.cisa.gov/known-exploited-vulnerabilities-catalog>

Latest Developments March 26, 2024: FortiGuard Labs continue to see attack attempts targeting the CVE-2019-7256 and has an existing IPS signature to block any attack attempts, however, it is recommended to apply firmware patch as recommended by the vendor to mitigate any risks fully.

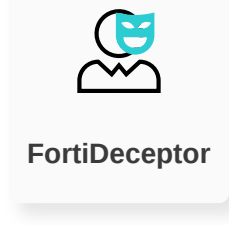
Since January of this year, the IPS signature designed to safeguard against CVE-2019-7256 has been intercepting attack attempts, blocking such incidents on around 1000 distinct IPS devices daily.

PROTECT

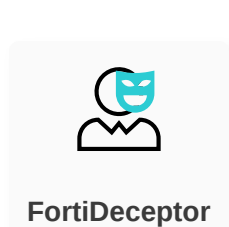
Countermeasures across the security fabric for protecting assets, data and network from cybersecurity events:

Reconnaissance

Lure



Decoy VM



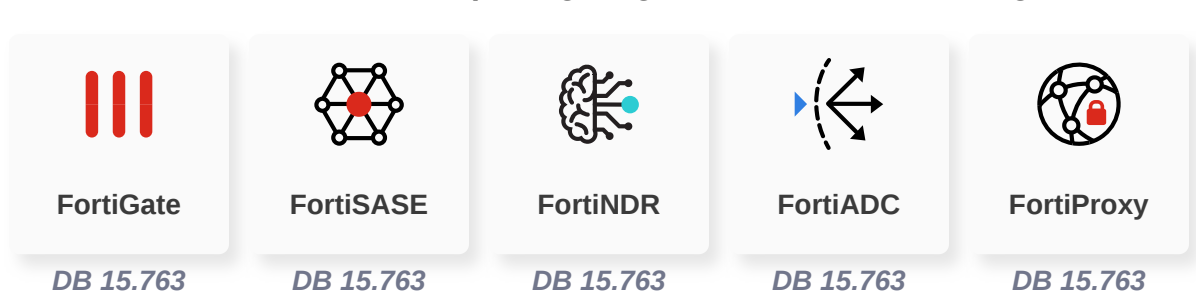
Weaponization

Delivery

Exploitation

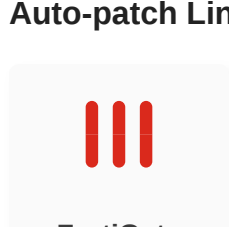
IPS

Detect and block attack attempts targeting vulnerable Linear eMerge E3-Series



IoT/IoT Virtual Patch

Auto-patch Linear eMerge Command Injection Vulnerability (CVE-2019-7256)



Installation

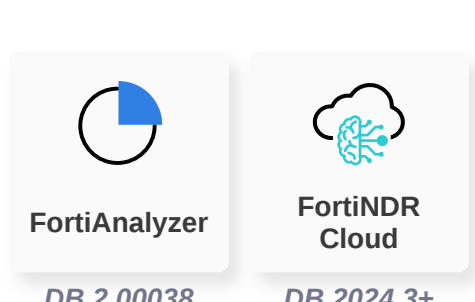
C2

Action

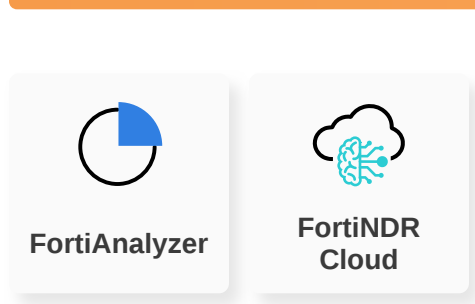
DETECT

Find and correlate important information to identify an outbreak, the following updates are available to raise alert and generate reports:

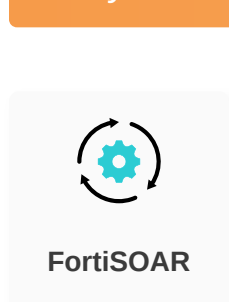
Outbreak Detection



Threat Hunting



Playbook

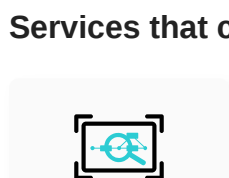


RESPOND

Develop containment techniques to mitigate impacts of security events:

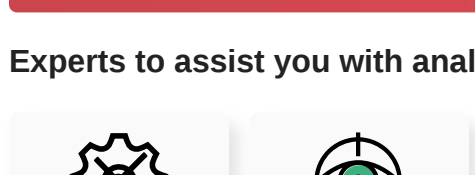
Automated Response

Services that can automatically respond to this outbreak.



Assisted Response Services

Experts to assist you with analysis, containment and response activities.

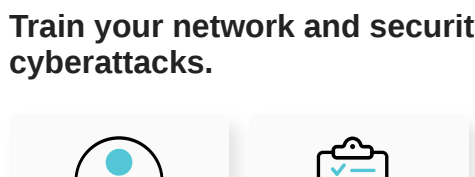


RECOVER

Improve security posture and processes by implementing security awareness and training, in preparation for (and recovery from) security incidents:

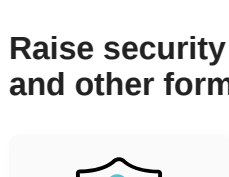
NOC/SOC Training

Train your network and security professionals and optimize your incident response to stay on top of the cyberattacks.



End-User Training

Raise security awareness to your employees that are continuously being targeted by phishing, drive-by download and other forms of cyberattacks.



IDENTIFY

Identify processes and assets that need protection:

Attack Surface Hardening

Check Security Fabric devices to build actionable configuration recommendations and key indicators.



Inventory Management

Check Security Fabric devices to build actionable configuration recommendations and key indicators.



Business Reputation

Know attackers next move to protect against your business branding.



Additional Resources

- CISA Advisory** <https://www.cisa.gov/news-events/ics-advisories/icsa-24-065-01>
- Security Week** <https://www.securityweek.com/exploited-building-access-system-vulnerability-patched-years-after-disclosure/>
- Medium** <https://medium.com/@scottbolena/a-backdoor-in-the-building-unveiling-the-nice-linear-emerge-e3-series-os-command-injection-fdb7d4016ef3>

Learn more about [FortiGuard Outbreak Alerts](#)