America's Cyber Defense Agency

NATIONAL COORDINATOR FOR CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE

Archived Content

In an effort to keep CISA.gov current, the archive contains outdated information that may not reflect current policy or programs.

ICS ADVISORY

Nordex NC2 XSS Vulnerability

Last Revised: August 27, 2018 **Alert Code:** ICSA-15-286-01

OVERVIEW

Independent researcher Karn Ganeshen has identified a cross-site scripting vulnerability in Nordex's NC2 Wind Farm Portal application. Nordex has produced an update to mitigate this vulnerability.

This vulnerability could be exploited remotely.

AFFECTED PRODUCTS

The following Nordex NC2 versions are affected:

- Nordex Control 2 (NC2) SCADA V16 and prior versions.

IMPACT

Cross-site scripting presents one entry point for attackers to access and manipulate control systems networks. It takes advantage of web servers that return dynamically generated web pages. Cross-site scripting also allows users to post viewable content in order to execute arbitrary HTML and active content such as JavaScript, ActiveX, and VBScript on a remote machine browsing the site within the context of a client-server session. This potentially allows the attacker to redirect the web page to a malicious location, hijack the client-server session, engage in network reconnaissance, and plant backdoor programs. Please refer to the ICS-CERT Abstract on Cross-Site Scripting for more information and additional mitigations.

Impact to individual organizations depends on many factors that are unique to each organization. NCCIC/ICS-CERT recommends that organizations evaluate the impact of this vulnerability based on their operational environment, architecture, and product implementation.

BACKGROUND

Nordex is a company based in Germany that maintains offices in countries around the world.

The affected product, Nordex Control 2, is a web-based SCADA system for wind power plants. According to Nordex, NC2 is deployed across the Energy sector. Nordex estimates that this product is used primarily in the United States, Europe, and China.

VULNERABILITY CHARACTERIZATION

VULNERABILITY OVERVIEW

CROSS-SITE SCRIPTINGCWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting'), http://cwe.mitre.org/data/definitions/79.html, web site last accessed October 13, 2015.

Cross-site scripting allows a malicious party to alter the pages presented by a web server such that other client browsers could be redirected to another page or download malicious script.

CVE-2015-6477NVD, http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-6477, NIST uses this advisory to create the CVE web site report. This web site will be active sometime after publication of this advisory. has been assigned to this vulnerability. A CVSS v3 base score of 6.1 and a temporal score of 5.5 have been assigned; the CVSS vector string is (AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N/E:P/RL:O/RC:C).CVSS Calculator, https://www.first.org/cvss/calculator/3.0#CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N/E:P/RL:O/RC:C, web site last accessed October 13, 2015.

VULNERABILITY DETAILS

EXPLOITABILITY

This vulnerability could be exploited remotely.

EXISTENCE OF EXPLOIT

No known public exploits specifically target this vulnerability.

DIFFICULTY

An attacker with a low skill would be able to exploit this vulnerability.

MITIGATION

The patching of the NC2-SCADA system has to be done by Nordex. Nordex will upgrade all wind farms with a valid service contract to the patched version of the NC2-SCADA in coordination with normal maintenance operations. Owners of Nordex NC2-based wind farms without a valid service contract can order the patch from Nordex by contacting their local Nordex service organization.

ICS-CERT recommends that users take defensive measures to minimize the risk of exploitation of these vulnerabilities. Specifically, users should:

- Minimize network exposure for all control system devices and/or systems, and ensure that they are not accessible from the Internet.
- Locate control system networks and remote devices behind firewalls, and isolate them from the business network.
- When remote access is required, use secure methods, such as Virtual Private Networks (VPNs), recognizing that VPNs may have vulnerabilities and should be updated to the most current version available. Also recognize that VPN is only as secure as the connected devices.

ICS-CERT reminds organizations to perform proper impact analysis and risk assessment prior to deploying defensive measures.

ICS-CERT also provides a section for control systems security recommended practices on the ICS-CERT web page at: http://ics-cert.us-cert.gov/content/recommended-practices </ics/content/recommended-practices>. Several recommended practices are available for reading and download, including Improving Industrial Control Systems Cybersecurity with Defense-in-Depth Strategies. </sites/default/files/recommended_practices/nccic_ics-cert_defense_in_depth_2016_s508c.pdf>

Additional mitigation guidance and recommended practices are publicly available in the ICS-CERT Technical Information Paper, ICS-TIP-12-146-01B--Targeted Cyber Intrusion Detection and Mitigation Strategies </ics/tips/ics-tip-12-146-01b>, that is available for download

from the ICS-CERT web site (http://ics-cert.us-cert.gov/ </ics/>).

Organizations observing any suspected malicious activity should follow their established internal procedures and report their findings to ICS-CERT for tracking and correlation against other incidents.

This product is provided subject to this Notification </notification> and this Privacy & Use </privacy-policy> policy.

Vendor

- Nordex

Please share your thoughts

We recently updated our anonymous product survey; we welcome your feedback.

Return to top

Topics </topics> **Spotlight** </spotlight> **Resources & Tools** </resources-tools>

News & Events </news-events> **Careers** </careers> **About** </about>

CYBERSECURITY &

INFRASTRUCTURE SECURITY AGENCY

CISA Central

1-844-Say-CISA contact@cisa.dhs.gov

CISA.gov
An official website of the U.S. Department of Homeland Security