

UNCLASSIFIED

24 August 2015



NORTH DAKOTA HOMELAND SECURITY Cyber Summary



The North Dakota Open Source Cyber Summary is a product of the North Dakota State and Local Intelligence Center (NDSLIC). It provides open source news articles and information on terrorism, crime, and potential destructive or damaging acts of nature or unintentional acts. Articles are placed in the Cyber Summary to provide situational awareness for local law enforcement, first responders, government officials, and private/public infrastructure owners.

UNCLASSIFIED

NDSLIC DISCLAIMER

The Cyber Summary is a non-commercial publication intended to educate and inform. Further reproduction or redistribution is subject to original copyright restrictions. NDSLIC provides no warranty of ownership of the copyright, or accuracy with respect to the original source material.

TABLE OF CONTENTS

[Regional](#)..... 3

[National](#)..... 3

[International](#)..... 3

[Banking and Finance Industry](#)..... 3

[Chemical and Hazardous Materials Sector](#)..... 3

[Commercial Facilities](#)..... 4

[Communications Sector](#)..... 4

[Critical Manufacturing](#)..... 4

[Defense/ Industry Base Sector](#)..... 5

[Emergency Services](#)..... 5

[Energy](#)..... 5

[Food and Agriculture](#)..... 5

[Government Sector \(including Schools and Universities\)](#)..... 5

[Information Technology and Telecommunications](#)..... 6

[US-Cert Updates and Vulnerabilities](#)..... 7

[ICS-Cert Alerts & Advisories](#)..... 7

[Public Health](#)..... 8

[Transportation](#)..... 8

[Water and Dams](#)..... 8

[North Dakota Homeland Security Contacts](#)..... 9

NORTH DAKOTA

Nothing Significant to Report

REGIONAL

Nothing Significant to Report

NATIONAL

Nothing Significant to Report

INTERNATIONAL

(International) Alerts issued for zero-day flaws in SCADA systems. The Industrial Control Systems Computer Emergency Response Team (ICS-CERT) published six advisories after security researchers from Elastica discovered several remote and local file inclusion, weak password hashing, insecure authentication, hardcoded credentials, weak cryptography, and cross-site request forgery (CSRF) vulnerabilities, among others, affecting Web-based Supervisory Control and Data Acquisition (SCADA) human machine interfaces (HMI) used by multiple organizations.

<http://www.securityweek.com/ics-cert-issues-alerts-zero-day-flaws-scada-systems>

BANKING AND FINANCE INDUSTRY

Nothing Significant to Report

CHEMICAL AND HAZARDOUS MATERIALS SECTOR

Nothing Significant to Report

COMMERCIAL FACILITIES

(National) Target settles Visa card issuer claims in breach. Target Corp., agreed to pay Visa Inc., up to \$67 million August 18 to resolve financial claims related to a 2013 data breach at Target that compromised the credit card information of at least 40 million customers over a 3-week period. Target has reported \$252 million in expenses tied to the breach to-date.

<http://www.startribune.com/target-settles-visa-card-issuer-claims-in-breach/322178271/>

COMMUNICATIONS SECTOR

Nothing Significant to Report

CRITICAL MANUFACTURING

(International) OwnStar attack now aimed at BMW, Chrysler, Mercedes cars. A security researcher who developed a Raspberry Pi-based device to intercept traffic between GM vehicles and the OnStar RemoteLink app reported that BMW, Mercedes-Benz, and Chrysler vehicles were also vulnerable to attacks due to similar respective mobile app failures to validate Secure Sockets Layer (SSL) certificates.

<https://threatpost.com/ownstar-attack-now-aimed-at-bmw-chrysler-mercedes-cars/114283>

(International) Security flaw affecting more than 100 car models exposed by scientists. Research published from a 2013 report by British and Dutch academics revealed weaknesses in the Swiss-made Megamos Crypto system used to prevent certain Audi, Citroën, Fiat, Honda, Volvo, and Volkswagen vehicles' engines from starting when a remote key is not present, in which a third party could use "close-range wireless communication" attacks to disable the system and steal the vehicle.

<http://www.theguardian.com/technology/2015/aug/18/security-flaw-100-car-models-exposed-scientists-volkswagen-suppressed-paper>

DEFENSE/ INDUSTRY BASE SECTOR

Nothing Significant to Report

EMERGENCY SERVICES

Nothing Significant to Report

ENERGY

Nothing Significant to Report

FOOD AND AGRICULTURE

Nothing Significant to Report

GOVERNMENT SECTOR (INCLUDING SCHOOLS AND UNIVERSITIES)

(Virginia) UVA board hears about cyberattack, faculty hiring progress. University of Virginia officials restored the school's computer network August 16 after shutting it down August 14 due to a cyber-security threat that targeted the personal email accounts of 2 university employees. Faculty, students, and staff were urged to change their passwords after the network was brought back online. http://www.dailyprogress.com/news/local/uva-board-hears-about-cyberattack-faculty-hiring-progress/article_6c8046fc-4472-11e5-9b22-3b3cfa4ab569.html

(National) IRS Raises Estimate of Taxpayer Files Breached. US authorities said Monday a breach of taxpayer records was more extensive than originally estimated, and that some 300,000 accounts appear now to have been affected. The agency said in May the breach affected some 100,000 taxpayer accounts <http://www.securityweek.com/irs-raises-estimate-taxpayer-files-breached>

UNCLASSIFIED

(Colorado) Colorado's OIT notifies 3,000 residents of data breach. Over 3,000 residents were notified by Colorado's Office of Information Technology (OIT) August 17 after a technical error resulted in letters containing the residents' personal, financial, and medical information being mailed to the wrong address between May and June. The OIT fixed the issue and implemented additional quality control checks. <http://www.scmagazine.com/colorados-oit-notifies-3000-residents-of-data-breach/article/433888/>

(Rhode Island) URI says data breach involves some 3,000 email accounts. The FBI is assisting August 20 in an investigation into a breach of the University of Rhode Island's email account records, which would have given hackers access to the email addresses and passwords of about 3,000 university email accounts. School officials stated that thieves may have also gained access to students' private email account passwords. <http://www.providencejournal.com/article/20150820/NEWS/150829905>

INFORMATION TECHNOLOGY AND TELECOMMUNICATIONS

(International) Administrators continue to fail in securing databases by using proper configs. Security researchers from BinaryEdge released analysis of 4 technologies including Redis, MongoDB, Memcached, and Elasticsearch, revealing that almost 1.2 petabytes (PB), or 1,175 terabytes (TB) of data were vulnerable due to administrators' use of default configurations that do not block connections from untrusted external actors. <http://news.softpedia.com/news/administrators-continue-to-fail-in-securing-databases-by-using-proper-configs-489322.shtml>

(International) Compromising details on thousands of military personnel have reportedly been leaked in the huge Ashley Madison hack. Highly compromising data on millions of people was leaked online on Tuesday, following the hack of extra-marital affairs dating website Ashley Madison in July. It includes everything from email addresses and financial information to sexual fantasies. In short, it's a blackmailer's paradise. There are 6,788 us.army.mil addresses, for example, another 1,665 navy.mil ones, and 809 usmc.mil. <http://www.msn.com/en-us/news/technology/compromising-details-on-thousands-of-military-personnel-have-reportedly-been-leaked-in-the-huge-ashley-madison-hack/ar-BBIRnfQ>

UNCLASSIFIED

(International) Emergency IE patch fixes vulnerability under attack. Microsoft released an emergency patch August 18 for all supported versions of its Internet Explorer Web browser addressing a zero-day memory corruption vulnerability that an attacker could leverage to remotely execute arbitrary code in the context of the current user.

<https://threatpost.com/emergency-ie-patch-fixes-vulnerability-under-attack/114342>

(International) New Data Leaked From 'Cheater' Site Ashley Madison. Hackers released what was purported to be a second batch of data from the affair-seeker website Ashley Madison. Coming two days after the release of some 32 million emails and user account information, the second leak appeared to contain internal company files and emails.

<http://www.securityweek.com/new-data-leaked-cheater-site-ashley-madison>

US-CERT UPDATES AND VULNERABILITIES

(International) Cisco Prime Infrastructure contains SUID root binaries. The Cisco Prime Infrastructure version 2.2 contains two binaries with SUID root world-executable privileges, allowing any local user to execute arbitrary commands as root.

<http://www.kb.cert.org/vuls/id/300820>

(International) Trend Micro Deep Discovery threat appliance contains multiple vulnerabilities. The Trend Micro Deep Discovery platform "enables you to detect, analyze, and respond to today's stealthy, targeted attacks in real time." It may be deployed on a network as an appliance. The Trend Micro Deep Discovery Threat Appliance version 3.7.1096 is vulnerable to cross-site scripting and authentication bypass.

<http://www.kb.cert.org/vuls/id/248692>

ICS-CERT ALERTS & ADVISORIES

Nothing Significant to Report

PUBLIC HEALTH

Nothing Significant to Report

TRANSPORTATION

Nothing Significant to Report

WATER AND DAMS

Nothing Significant to Report

NORTH DAKOTA HOMELAND SECURITY CONTACTS

To report a homeland security incident, please contact your local law enforcement agency or one of these agencies: **North Dakota State and Local Intelligence Center:** 866-885-8295(IN ND ONLY); Email: ndslic@nd.gov; Fax: 701-328-8175 **State Radio:** 800-472-2121; **Bureau of Criminal Investigation (BCI):** 701-328-5500; **North Dakota Highway Patrol:** 701-328-2455; **US Attorney's Office Intel Analyst:** 701-297-7400; **Bismarck FBI:** 701-223-4875; **Fargo FBI:** 701-232-7241.

To contribute to this summary or if you have questions or comments, please contact:

Darin Hanson, ND Division of Homeland Security dthanson@nd.gov, 701-328-8165