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In an effort to keep CISA.gov current, the archive contains outdated information that may not reflect current policy or programs.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

# Philips Intellispace Portal ISP Vulnerabilities

**Last Revised:** February 27, 2018 **Alert Code:** ICSMA-18-058-02

## OVERVIEW

Philips reported vulnerabilities in the Philips' IntelliSpace Portal (ISP), an advanced visualization and image analysis system. Philips is creating a software update to mitigate these vulnerabilities in the affected products. Additionally, they are issuing mitigating controls for some vulnerabilities.

Some vulnerabilities could be exploited remotely.

Exploits that target some vulnerabilities are publicly available.

## AFFECTED PRODUCTS

Philips reports that these vulnerabilities affect the following versions of the ISP:

- IntelliSpace Portal, all 8.0.x versions, and
- IntelliSpace Portal, all 7.0.x versions.

# IMPACT

Successful exploitation of these vulnerabilities could allow an attacker to gain unauthorized access to sensitive information, perform man-in-the-middle attacks, create denial of service conditions, or execute arbitrary code.

Impact to individual organizations depends on many factors that are unique to each organization. NCCIC recommends that organizations evaluate the impact of these vulnerabilities based on their operational environment and specific clinical usage.

# BACKGROUND

Philips is a global company that maintains offices in many countries around the world, including countries in Africa, Asia, Europe, Latin America, the Middle East, and North America.

The Philips ISP processes clinical images from different modalities and enables advanced visualization of the images. ISP systems are deployed across the Healthcare and Public Health sectors. Philips estimates these products are used worldwide.

# VULNERABILITY CHARACTERIZATION

## VULNERABILITY OVERVIEW

### IMPROPER INPUT VALIDATION CWE-20 <https://cwe.mitre.org/data/definitions/20.html>

The ISP has multiple input validation vulnerabilities that could allow a remote attacker to execute arbitrary code or cause the application to crash.

CVE-2018-5474 <https://nvd.nist.gov/vuln/detail/cve-2018-5474>, CVE-2017-0143 <https://nvd.nist.gov/vuln/detail/cve-2017-0143>, CVE-2017-0144 <https://nvd.nist.gov/vuln/detail/cve-2017-0144>, CVE-2017-0145 <https://nvd.nist.gov/vuln/detail/cve-2017-0145>, CVE-2017-0146 <https://nvd.nist.gov/vuln/detail/cve-2017-0146>, CVE-2017-0148 <https://nvd.nist.gov/vuln/detail/cve-2017-0148>, CVE-2017-0272 <https://nvd.nist.gov/vuln/detail/cve-2017-0272>, CVE-2017-0277 <https://nvd.nist.gov/vuln/detail/cve-2017-0277>, CVE-2017-0278 <https://nvd.nist.gov/vuln/detail/cve-2017-0278>, CVE-2017-0279 <https://nvd.nist.gov/vuln/detail/cve-2017-0279>, CVE-2017-0269 <https://nvd.nist.gov/vuln/detail/cve-2017-0269>, CVE-2017-0273 <https://nvd.nist.gov/vuln/detail/cve-2017-0273>, and CVE-2017-0280 <https://nvd.nist.gov/vuln/detail/cve-2017-0280> have been assigned to these vulnerabilities. The CVSS v3 base scores for theses vulnerabilities range from 5.9 to 8.1

## INFORMATION EXPOSURE CWE-200 <https://cwe.mitre.org/data/definitions/200.html>

The ISP has multiple information exposure vulnerabilities that could allow an attacker to gain unauthorized access to sensitive information.

CVE-2017-0147, CVE-2017-0267 <https://nvd.nist.gov/vuln/detail/cve-2017-0267>, CVE-2017-0268 <https://nvd.nist.gov/vuln/detail/cve-2017-0268>, CVE-2017-0270 <https://nvd.nist.gov/vuln/detail/cve-2017-0270>, CVE-2017-0271 <https://nvd.nist.gov/vuln/detail/cve-2017-0271>, CVE-2017-0274 <https://nvd.nist.gov/vuln/detail/cve-2017-0274>, CVE-2017-0275 <https://nvd.nist.gov/vuln/detail/cve-2017-0275>, and CVE-2017-0276 <https://nvd.nist.gov/vuln/detail/cve-2017-0276>, have been assigned to these vulnerabilities. A CVSS v3 base score of 5.9 has been calculated; the CVSS vector string is (AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N <https://www.first.org/cvss/calculator/3.0#cvss:3.0/av:n/ac:h/pr:n/ui:n/s:u/c:h/i:n/a:n>).

## PERMISSIONS, PRIVILEGES, AND ACCESS CONTROLS CWE-264 <https://cwe.mitre.org/data/definitions/264.html>

The ISP has multiple permission, privilege and access control vulnerabilities that could allow an attacker to gain unauthorized access and in some cases escalate their level of privilege or execute arbitrary code.

CVE-2018-5472, CVE-2018-5468 <https://nvd.nist.gov/vuln/detail/cve-2018-5468>, CVE-2017-0199 <https://nvd.nist.gov/vuln/detail/cve-2017-0199>, and CVE-2005-1794 <https://nvd.nist.gov/vuln/detail/cve-20005-1794> have been assigned to this vulnerability. The CVSS v3 base scores for theses vulnerabilities range from 6.4 to 7.8

## UNQUOTED SEARCH PATH OR ELEMENT CWE-428

<https://cwe.mitre.org/data/definitions/428.html>

An unquoted search path or element vulnerability has been identified, which may allow an authorized local user to execute arbitrary code and escalate their level of privileges.

CVE-2018-5470, has been assigned to this vulnerability. A CVSS v3 base score of 7.8 has been calculated; the CVSS vector string is (AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H <https://www.first.org/cvss/calculator/3.0#cvss:3.0/av:l/ac:l/pr:l/ui:n/s:u/c:h/i:h/a:h>).

## LEFTOVER DEBUG CODE CWE-489 <https://cwe.mitre.org/data/definitions/489.html>

The ISP has a vulnerability where code debugging methods are enabled, which could allow an attacker to remotely execute arbitrary code during runtime.

CVE-2018-5454 has been assigned to this vulnerability. A CVSS v3 base score of 5.3 has been calculated; the CVSS vector string is (AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N <https://www.first.org/cvss/calculator/3.0#cvss:3.0/av:n/ac:l/pr:n/ui:n/s:u/c:n/i:l/a:n>).

## CRYPTOGRAPHIC ISSUES CWE-310 <https://cwe.mitre.org/data/definitions/310.html>

The ISP has multiple cryptographic vulnerabilities that could allow an attacker to gain unauthorized access to resources and information.

CVE-2018-5458, CVE-2018-5462 <https://nvd.nist.gov/vuln/detail/cve-2018-5462>, CVE-2018-5464 <https://nvd.nist.gov/vuln/detail/cve-2018-5464>, CVE-2018-5466 <https://nvd.nist.gov/vuln/detail/cve-2018-5466>, CVE-2011-3389 <https://nvd.nist.gov/vuln/detail/cve-2011-3389>, CVE-2004-2761 <https://nvd.nist.gov/vuln/detail/cve-2004-2761>, CVE-2014-3566 <https://nvd.nist.gov/vuln/detail/cve-

2014-3566>, and CVE-2016-2183 <https://nvd.nist.gov/vuln/detail/cve-2016-2183> have been assigned to these vulnerabilities. The CVSS v3 base scores for theses vulnerabilities range from 3.1 to 6.5

### VULNERABILITY DETAILS

### EXPLOITABILITY

Some vulnerabilities could be exploited remotely.

### EXISTENCE OF EXPLOIT

Public exploits exist for some of these vulnerabilities; however, none are known to specifically target Philips ISP.

### DIFFICULTY

An attacker with a low skill would be able to exploit these vulnerabilities.

## MITIGATION

Philips will release an updated version of the ISP in the coming months that will address these vulnerabilities. Additionally, Philips' evaluation of Operating System security patches is ongoing, and after appropriate testing , the patches and mitigating controls are posted on Philips' InCenter. ISP users are recommended to obtain available mitigating controls by accessing their InCenter account at this location:

http://incenter.medical.philips.com <http://incenter.medical.philips.com>

Users with questions regarding their specific ISP installations are advised by Philips to contact their local Philips service support team or their regional service support.

Philips' contact information is available at the following location:

https://www.usa.philips.com/healthcare/solutions/customer-service-solutions <https://www.usa.philips.com/healthcare/solutions/customer-service-solutions>

Please see the Philips product security website for the latest security information for Philips products:

https://www.philips.com/productsecurity <https://www.philips.com/productsecurity>

NCCIC recommends 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 </ics/alerts/ics-alert-10-301-01>.
- Locate all medical devices 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.

NCCIC also provides a section for control systems security recommended practices </ics/content/recommended-practices> on the ICS-CERT web page. NCCIC reminds organizations to perform proper impact analysis and risk assessment prior to deploying defensive measures.

Additional mitigation guidance and recommended practices are publicly available in the NCCIC 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 website </ics/>.

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

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

# Vendor

- Philips

## 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